



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

**ANÁLISIS E IMPACTO DEL REGLAMENTO GENERAL DE
PROTECCIÓN DE DATOS. APLICACIÓN AL SECTOR DE LA
ELECTRÓNICA DE CONSUMO**

Trabajo Fin de Grado presentado por Pablo González González, siendo el tutor del mismo el profesor José Carlos Ruiz del Castillo.

Vº. Bº. del Tutor:

Alumno:

D. José Carlos Ruiz del Castillo

D. Pablo González González

Sevilla, Julio de 2018



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES
GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FIN DE GRADO
CURSO ACADÉMICO [2017-2018]

TÍTULO: ANÁLISIS E IMPACTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. APLICACIÓN AL SECTOR DE LA ELECTRÓNICA DE CONSUMO

AUTOR: PABLO GONZÁLEZ GONZÁLEZ

TUTOR: JOSÉ CARLOS RUIZ DEL CASTILLO

DEPARTAMENTO: ECONOMÍA FINANCIERA Y DIRECCIÓN DE OPERACIONES

ÁREA DE CONOCIMIENTO: ORGANIZACIÓN DE EMPRESAS

RESUMEN:

La protección de datos está tomando cada vez un papel más importante en la sociedad. Su relevancia ha ido creciendo en los últimos años, hasta el punto en que, actualmente, es tema principal en usuarios y todo tipo de organizaciones. El presente trabajo, estimulado por la entrada en vigor y plena aplicación del Reglamento General de Protección de Datos, estudia la evolución de este derecho fundamental en España, iniciándonos en su entendimiento y analizando su situación actual y próxima.

Para ello, se hará un breve repaso en el tiempo sobre la normativa reguladora de este aspecto en nuestro país, hasta llegar al anteriormente citado Reglamento. En él, nos detendremos para analizar detalladamente su contenido y, especialmente, las novedades que presenta respecto a legislaciones anteriores. Punto de inflexión para toda empresa de ámbito europeo, comprobaremos mediante un estudio el grado de cumplimiento o adaptación de un determinado sector a esta nueva normativa, llena de cambios y tras un margen de dos años para satisfacerlos.

TÉRMINOS CLAVE:

Protección de datos; Reglamento General de Protección de datos; RGPD; LOPD; Cumplimiento RGPD.

ÍNDICE

| | | |
|----------|---|-----------|
| 1 | INTRODUCCIÓN..... | 7 |
| 1.1 | INTRODUCCIÓN Y JUSTIFICACIÓN | 7 |
| 1.2 | OBJETIVOS PROPUESTOS..... | 9 |
| 1.2.1 | OBJETIVO GENERAL | 9 |
| 1.2.2 | OBJETIVOS ESPECÍFICOS..... | 9 |
| 1.3 | METODOLOGÍA..... | 10 |
| 1.4 | ESTRUCTURA DEL TRABAJO..... | 12 |
| 2 | LA PROTECCIÓN DE DATOS | 13 |
| 2.1 | INTIMIDAD, PRIVACIDAD Y PROTECCIÓN DE DATOS..... | 13 |
| 2.2 | DEFINICIÓN E HITOS HISTÓRICOS..... | 14 |
| 3 | MARCO LEGAL | 19 |
| 3.1 | REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS..... | 19 |
| 3.1.1 | CONSIDERACIONES INICIALES..... | 20 |
| 3.1.2 | ETAPAS, JUSTIFICACIÓN Y OBJETIVOS | 21 |
| 3.1.3 | CONTENIDO PRINCIPAL Y NOVEDADES..... | 25 |
| 3.1.4 | REFUERZO DE LA TRANSPARENCIA Y EL CONSENTIMIENTO..... | 37 |
| 3.2 | PROYECTO DE NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS..... | 40 |
| 3.2.1 | ETAPAS Y SITUACIÓN ACTUAL | 41 |
| 3.2.2 | DIFERENCIAS Y ADAPTACIÓN AL NUEVO RGPD/LOPD | 41 |
| 4 | ESTUDIO DEL GRADO DE CUMPLIMIENTO DEL RGPD EN EL SECTOR DE LA ELECTRÓNICA DE CONSUMO EN ESPAÑA | 43 |
| 4.1 | METODOLOGÍA Y LIMITACIONES..... | 43 |
| 4.2 | SELECCIÓN DE LA MUESTRA..... | 45 |

| | | |
|-----|---|----|
| 4.3 | ELABORACIÓN DE LA LISTA DE CONTROL..... | 47 |
| 4.4 | REALIZACIÓN DEL ESTUDIO | 49 |
| 5 | CONCLUSIONES | 61 |
| 6 | BIBLIOGRAFÍA | 63 |

Relación de Figuras

| | |
|--|----|
| Figura 3.1. Artículo 99 RGPD | 21 |
| Figura 3.2. Derechos ARCO según AEPD | 30 |
| Figura 3.3. Información por capas..... | 40 |
| Figura 4.1. Búsqueda del término “comprar informática” | 46 |
| Figura 4.2. Búsqueda del término “comprar ordenadores portátiles” | 46 |
| Figura 4.3. Búsqueda del término “comprar smartphones ordenadores en Sevilla” | 47 |
| Figura 4.4. Política de Privacidad de PcComponentes | 50 |
| Figura 4.5. Obtención del consentimiento de PcComponentes..... | 51 |
| Figura 4.6. Política de Privacidad de Ecomputer | 52 |
| Figura 4.7. Obtención del consentimiento de Ecomputer..... | 52 |
| Figura 4.8. Seguimiento del proceso de obtención del consentimiento de Ecomputer... 53 | |
| Figura 4.9. Política de Privacidad de Fnac | 54 |
| Figura 4.10. Delegado de Protección de Datos de Fnac..... | 55 |
| Figura 4.11. Obtención del consentimiento de Fnac..... | 55 |
| Figura 4.12. Política de Privacidad de Tecnican | 56 |
| Figura 4.13. Obtención del consentimiento de Tecnican..... | 57 |
| Figura 4.14. Política de Privacidad de Mleón | 58 |
| Figura 4.15. Obtención del consentimiento de Mleón..... | 59 |

Relación de Tablas

| | |
|---|----|
| Tabla 3-1. Novedades y sus artículos | 27 |
| Tabla 3-2. Tipos de sanciones y cuantías en LOPD y RGPD | 37 |

1 INTRODUCCIÓN

1.1 INTRODUCCIÓN Y JUSTIFICACIÓN

Las tecnologías de la información y comunicación (TIC) son, sin duda, principales protagonistas de las últimas dos décadas, precursoras de este entorno tan dinámico que nos rodea, con una cantidad y velocidad de cambios vertiginosa. El descubrimiento y desarrollo de nuevas tecnologías y la propagación inmediata de la información, accesibles a la gran mayoría de ámbitos sociales y regiones, han modificado por completo las pautas de comportamiento y forma de vivir.

Las TIC tienen en Internet su mayor aliado. Es difícil imaginar y entender, por no decir imposible, todo este desarrollo sin su existencia. Internet ha revolucionado las comunicaciones y se ha convertido en la fuente de información, conocimiento y entretenimiento más amplia y usada de la historia. Ha abierto un mundo de posibilidades a todos los niveles, el cual crece día a día al igual que su número de usuarios.

Ante este contexto, resulta inconcebible ponerle límites a la cantidad de información y datos que circula por Internet. Dentro de la compleja tipología de los datos, el presente trabajo se centrará en los datos personales.

Los datos personales son, según el Reglamento General de Protección de Datos, toda información sobre una persona física identificada o identificable. Es decir, permiten identificar a una persona, desde un apellido hasta el número de matrícula del coche. Los usuarios rara vez realizan en Internet alguna actividad o gestión sin dejar rastro de sus datos. Procesos como comprar en una tienda online o registrarse en un foro, dejan a sus espaldas numerosos datos que pueden comprometer al usuario si se les da un uso fraudulento.

Si este mundo de posibilidades que ofrece Internet ha supuesto un progreso en la sociedad y un aumento de la calidad de vida de la población incalculable, es en parte gracias a la comodidad y rapidez actual para la transmisión e intercambio de los citados datos. Por lo tanto, la búsqueda de un equilibrio entre modernización y privacidad del usuario resultaba necesaria. La Agencia Española de Protección de Datos [AEPD] (2005, p.6) señala:

“Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información es

el contexto en el que el legislador consagra el derecho fundamental a la protección de datos de carácter personal”.

La exposición de este derecho fundamental al siempre cambiante mundo tecnológico hace necesaria su continua revisión y adaptación, con el fin de no quedarse obsoleto y garantizar la seguridad de todos los ciudadanos. Así, son varias las leyes, reglamentos y directivas europeas que han velado por este derecho durante el transcurso de las últimas décadas, los cuales repasaremos posteriormente. En este trabajo fin de grado, nos centraremos en el Reglamento General de Protección de Datos (RGPD), normativa más reciente, proveniente de la Unión Europea y, por tanto, con influencia directa en España.

El RGPD, con fecha de plena aplicación el 25 de mayo de 2018, supone una serie de cambios importantes en la protección de datos. Las empresas, de todo tipo de tamaños y sectores, deben adecuarse a las nuevas exigencias y obligaciones, hecho que siempre provoca cierto revuelo por el desconocimiento y la confusión que se crea en los primeros compases, especialmente las pymes poseedoras de menores recursos.

Tras disponer las empresas de un período de 2 años para la aplicación del RGPD, creemos interesante la realización de un estudio que analice la respuesta de las organizaciones a estos cambios. Por lo tanto, en una primera razón o justificación del presente trabajo, la obtención de los resultados posibilitará deducir la influencia y efectividad de esta nueva normativa, contemplando en qué medida las empresas dan prioridad al buen hacer en el tratamiento de datos de carácter personal.

Asimismo, la adaptación al RGPD trae consigo diversas modificaciones que afectan a las políticas de las empresas y al diseño de sus páginas web, situación de adversidad para un número elevado de empresas con un presupuesto más limitado. Este hecho nos permitirá comprobar cómo hacen frente las organizaciones, especial mención a las pymes, a la consecución de lo dispuesto en el reglamento, cuestión de sumo interés académico y trascendental de cara a preservar su imagen y evitar duras sanciones.

La protección de datos es un tema de plena actualidad, lleno de retos y con una previsión que todo parece indicar seguirá aumentando su importancia en años venideros. Cada vez son más frecuentes en periódicos y telediarios noticias de fraudes con relación a esta disciplina, la mayoría pertenecientes a redes sociales como Facebook, webs con millones de usuarios reconocidas mundialmente cuyo pilar básico se sustenta en la recopilación y transmisión de datos personales.

Gracias a ello, los ciudadanos están incrementando progresivamente su grado de conocimiento y sensibilización en la materia, dejando de ser un aspecto ignorado o desconocido por la gran mayoría. Así pues, la relevancia actual y futura, tanto a nivel social como empresarial, junto al propio interés del alumno, constituyen una segunda justificación del presente trabajo fin de grado.

1.2 OBJETIVOS PROPUESTOS

Para la correcta realización de este trabajo fin de grado, se ha planteado una serie de objetivos que cumplir, clasificados en dos tipos:

1.2.1 OBJETIVO GENERAL

El principal objetivo de este trabajo es generar conocimiento acerca de todo lo que rodea al reglamento entrado en vigor, especialmente su incidencia y grado de adaptación por parte de empresas que actúan en España. La obligatoria perspectiva jurídica de un trabajo de tales características se complementará con una visión empresarial, acorde a nuestro ámbito de estudio.

1.2.2 OBJETIVOS ESPECÍFICOS

Desglosando el objetivo general, se extraen los siguientes objetivos específicos:

- Poner en contexto la protección de datos en España, un vistazo en el tiempo a su historia y normativa reguladora.
- Analizar el nuevo Reglamento General de Protección de Datos. Su fase de elaboración, circunstancias que han llevado a los órganos de la UE a su planteamiento y realización, además de los objetivos y metas previstas.
- Ser un documento que sirva de guía a empresas de cara a comprobar en qué medida están cumpliendo o no las obligaciones de la nueva normativa.
- Por otro lado, dar a conocer al ciudadano qué derechos le pertenecen en materia de protección de datos, tanto los nuevos contenidos en el RGPD como los ya existentes en la Ley Orgánica de Protección de Datos.
- Analizar el Proyecto de Nueva Ley Orgánica de Protección de Datos. En fase de aprobación por el Congreso, será la nueva legislación española adaptada a las directrices del reglamento europeo.
- Por último, se estudiará el cumplimiento de las disposiciones impuestas por la Unión Europea contenidas en el RGPD. Para ello, ante la imposibilidad lógica de analizar todas las empresas, se utilizará una muestra de un sector concreto, en este caso la electrónica de consumo.

1.3 METODOLOGÍA

Para la realización y cumplimiento de los objetivos del presente trabajo, se requería generar primeramente un amplio conocimiento sobre la materia, partiendo prácticamente desde cero. La principal herramienta para su consecución ha sido Internet. Este medio crece exponencialmente, lo cual sus posibilidades de encontrar información útil y de interés son prácticamente ilimitadas.

Lógicamente, ante tanta sobrecarga de información y en tanta diversidad de soportes, se le debe dar importancia a revisar su procedencia y veracidad. Por ello, es clave también es tener claro el rigor de la información obtenida. Para el desarrollo del presente trabajo se ha utilizado un sistema mixto, alternando el uso de buscadores genéricos y contenido menos riguroso, junto a búsquedas en portales bibliográficos que nos otorgaran publicaciones de mayor carácter académico.

Los primeros pasos del trabajo consistieron en la realización de búsquedas a través del **buscador genérico Google**, tratando de recabar información sobre el Reglamento General de Protección de Datos, tema central que nos ocupa. “Reglamento General de Protección de Datos”, “RGPD” y “nuevo reglamento protección de datos” fueron las búsquedas realizadas. Si bien el RGPD es simplemente una consecuencia de la evolución de toda una disciplina jurídica durante décadas, resultó ser nuestro punto de partida para el resto de la investigación. A través de los resultados de las búsquedas se revisaron noticias en periódicos y diversos blogs con el fin de crear un primer acercamiento a la materia. Estas fuentes no están reflejadas en el trabajo final, simplemente se utilizaron con fines de consulta.

Así, el próximo paso fue acudir a fuentes oficiales, necesarias para un mayor grado de rigor y detalle. Se revisó el Reglamento 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), además de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), ambos textos presentes en la web Boletín Oficial del Estado. La primera visión de estos textos produjo resultados poco solventes debido al bajo conocimiento de la materia y del ámbito jurídico en general.

Posteriormente, con el objetivo de obtener información igualmente formal pero que resultara más fácil su comprensión, se emplearon portales webs especializados en investigación como **Dialnet**, **Google Académico** y **Fama de la Universidad de Sevilla**. Se usaron para la búsqueda los mismos términos anteriormente citados “Reglamento General de Protección de Datos”, “RGPD” y “nuevo reglamento protección de datos”.

En las publicaciones escogidas se valoraba su generalidad y su lenguaje, es decir, que trataran el Reglamento en su conjunto y no un aspecto determinado dentro de él, y en un lenguaje no demasiado técnico.

Una herramienta fundamental en el desarrollo del TFG ha resultado ser la web de la **Agencia Española de Protección de Datos**, la cual tiene a disposición varias guías y recursos útiles relacionados con el nuevo Reglamento, en un formato y lenguaje más familiarizados con el ciudadano. La información encontrada en esta página web ha sido esencial durante todo el proceso, desde la primera asimilación de la materia, pasando a su posterior profundización hasta llegar al capítulo final del trabajo, donde resultó de gran ayuda para poner en práctica lo aprendido.

Debido a la necesidad de una introducción que precediera a todo el marco legal actual, con el propósito de entender su procedencia y aspectos que realmente regula, se realizaron búsquedas, tanto en Google como en los portales anteriormente citados, más generales acerca de la protección de datos. “La protección de datos”, “protección de datos derecho fundamental”, “Historia de la protección de datos personales” nos arrojaron centenares de resultados. Para su selección primó nuevamente el lenguaje utilizado, su clara redacción y la calidad del autor. Especial mención al profesor Juan Vicente Oltra Gutiérrez por sus videos en formato Polimedia y Álvaro Canales Gil por su obra “El derecho fundamental a la protección de datos de carácter personal”.

También ha resultado objeto de investigación el Proyecto de Ley Orgánica de Protección de Datos. Al ser una legislación aún en proceso, gran parte de la información disponible y utilizada se encuentra básicamente en periódicos online y portales jurídicos especializados, a excepción de los documentos oficiales encontrados en la web del Congreso o del ministerio de Justicia. “Proyecto de Ley Orgánica de Protección de Datos” fue la búsqueda de referencia, en la que primaron los resultados más recientes, de cara a conocer todo su proceso y situación actual.

Finalmente, con el objetivo de tratar la materia estudiada desde un punto de vista más práctico y real, que ponga en valor los conocimientos aprendidos por el alumno, será realizado un estudio del grado de adaptación de varias empresas seleccionadas a las nuevas exigencias que se imponen en el RGPD. El proceso consistirá en la verificación de la existencia de una serie de elementos contenidos previamente en una lista de control, en las páginas web de las empresas seleccionadas. El número de empresas elegidas suman un total de cinco, las cuales serán obtenidas por ser las mejores posicionadas en los resultados naturales (SEO) de varias búsquedas realizadas en Google sobre términos relacionados con el sector elegido, la electrónica de consumo, y

sus productos. Una explicación más detallada de la metodología empelada en este estudio se encuentra en el capítulo **Error! Reference source not found.**

1.4 ESTRUCTURA DEL TRABAJO

En el próximo capítulo introduciremos el concepto de la protección de datos. En primer lugar, se tratará su origen, siempre vinculado con los términos intimidad y privacidad, los cuales serán definidos y relacionados con la protección de datos, además de nombrar el principal desencadenante de su creación, la llegada de la informática. Posteriormente, se verá su definición, para continuar con un breve repaso por la historia de esta materia, tanto a nivel europeo como español, hasta llegar a nuestro contexto actual.

En el capítulo 3, nos detendremos en el reciente Reglamento General de Protección de Datos para analizar detalladamente sus novedades introducidas, especial mención a las modificaciones en la obtención del consentimiento y el refuerzo de la información y transparencia, con un subapartado dedicado. Anteriormente, en el primer subapartado se realizará un resumen y contexto inicial del Reglamento, para pasar en un segundo subapartado a su proceso de elaboración, causas y objetivos.

El capítulo 3 finaliza con un análisis del Proyecto de Ley Orgánica de Protección de Datos. Se desarrollará su contexto inicial, estado actual y adaptación al RGPD, además de diferencias respecto a la anterior Ley Orgánica de Protección de Datos española de 1999.

En el capítulo 4 se llevará a cabo el estudio del grado de cumplimiento del RGPD en el sector de la electrónica de consumo en España. Primeramente, será expuesta la metodología seguida y las limitaciones que han caracterizado y dado forma a este estudio. En los siguientes apartados serán vistos con mayor grado de detalle los procesos de selección de la muestra de empresas a estudiar y la elaboración de la lista de control. Para finalizar, será desarrollado el estudio y se comentarán varias conclusiones acerca de los resultados obtenidos.

2 LA PROTECCIÓN DE DATOS

La privacidad ha atesorado distintas concepciones a lo largo de la historia de la humanidad. Si bien en la antigua Grecia se priorizaba el colectivo y esta pasaba a ser ciertamente secundaria, es en la época romana cuando se empieza a diferenciar al hombre interior del hombre exterior. Esta evolución nos lleva a Santo Tomás en la Edad Media, quien reivindica que el hombre en su momento de rezo debe tener un momento de intimidad sagrado, o al filósofo Locke ya en la Edad Moderna, que reafirma la esfera íntima del ser humano, incluyendo a las mujeres. (Oltra, 2016)

2.1 INTIMIDAD, PRIVACIDAD Y PROTECCIÓN DE DATOS

Privacidad e intimidad. Dos conceptos similares y conectados entre sí, pero diferentes. Intimidad según la Real Academia Española se define: “Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia”, mientras que privacidad: “Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”. La intimidad es un concepto más profundo y restringido, abarca aspectos tales como creencias, pensamientos o vida sexual de la persona. La privacidad es un término más amplio, datos de una persona que de forma aislada no tienen excesiva relevancia, pero tomados en su conjunto pueden generar un perfil de su personalidad o necesidades. (Anciano, 2015)

La Ley Orgánica N°5 (1992, p.1) señala:

En tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Ambos conceptos también difieren en su régimen de protección. La intimidad es un derecho fundamental amparado por la Constitución Española de 1978 en los tres primeros párrafos de su artículo 18. No obstante, los datos privados no gozaban de igual protección. Aspectos privados de una persona como sus gustos o aficiones no suponían gran peligro, estaban limitados por el olvido, por la dificultad de almacenarlos y

procesarlos conjuntamente para crear una imagen y diagnóstico del individuo. Es la irrupción de la informática la que cambia todo, permitiendo el registro y fácil comunicación de estos datos y rompiendo los citados límites. Ante ello, resultaba necesario una protección para el ciudadano, una frontera que garantizara un equilibrio entre la seguridad de la esfera privada del individuo y la modernización sobrevenida.

En este contexto surge la materia de la protección de datos de carácter personal. Como base de toda la regulación española, se encuentra el párrafo cuarto del artículo 18 de la Constitución Española: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (Constitución Española, 1978, art.18.4). Es cuanto menos curioso que, ya en esos años, el legislador se preocupara por las negativas consecuencias que podría traer el mundo informatizado a la sociedad, siendo inverosímil imaginar todos los avances de hoy día.

El citado artículo se desarrollaría posteriormente, dando lugar a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Años más tarde aparecería su reglamento, prácticamente simultáneo a una nueva Ley Orgánica que haría derogar la LORTAD, además de directivas europeas y numerosas sentencias del Tribunal Constitucional que irían matizando este derecho, siempre vinculado al derecho a la intimidad y el honor, hasta su desprendimiento y consagración como derecho fundamental, tanto a nivel europeo como a nivel nacional. En el próximo apartado se tratará con más detenimiento la evolución y principales hitos históricos de la protección de datos, hasta llegar a nuestros días con la reciente entrada en vigor del Reglamento General de Protección de Datos.

En conclusión, todo lo íntimo es privado, pero no todo lo privado es íntimo. El elemento común que los relaciona con la protección de datos es el tratamiento de datos e información personal. El derecho fundamental a la protección de datos vela por todos los datos de carácter personal, incluido tanto íntimos como privados, creándose una esfera de triple protección. (“Intimidad, privacidad y protección de datos de carácter personal”, 2006

2.2 DEFINICIÓN E HITOS HISTÓRICOS

El derecho fundamental de protección de datos, según AEPD (2005, p.6) “reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos”. Véase el carácter “positivo” o facultativo de este derecho. El derecho dispone al ciudadano de un poder, la posibilidad de controlar, si quiere, sus datos y decidir sobre ellos. A diferencia de, por ejemplo, el derecho a la intimidad, este

no es una facultad o poder de la persona, sino una barrera o prohibición al resto de individuos.

El derecho a la intimidad trata de proteger un espacio, en este caso íntimo, de la intromisión o injerencia de terceros, de decidir quién puede o no puede participar de las acciones, de las decisiones, de todo lo acaecido en ese ámbito que pertenece a los sujetos por el mero hecho de ser personas. (Martínez de Pisón, 2016, p.412)

Ser informado de cuándo y porqué se tratan sus datos personales, acceder a los datos y, en caso necesario, el derecho a su modificación o supresión, además de la oposición al tratamiento de los mismos (AEPD, 2005) forman el conjunto de derechos base de la protección de datos que conocemos hoy día, claves para la comprensión de su ámbito y marco de actuación. Véase la clara relación que surge de estos preceptos, entre usuarios o consumidores (personas físicas) y organizaciones o empresas (principales autores del tratamiento de datos), siendo estos últimos los sujetos pasivos obligados a cooperar con las personas físicas de cara al cumplimiento de sus derechos.

La protección de datos es una materia en constante evolución desde sus inicios, más aún en el presente y con un futuro que no da señal alguna que este proceso vaya a llegar a su fin. Su fuerte vinculación a la informática, término quizás algo obsoleto que daría paso a las tecnologías de la información y la comunicación (TIC), junto a la expansión de la red Internet, han dotado a esta materia de un carácter cambiante y una necesidad de aprendizaje y adaptación continuas.

En páginas anteriores nos hemos referido a la protección de datos de carácter personal como un derecho fundamental, pero ¿Desde cuándo lo es? ¿Está también reconocido en el Derecho Comunitario Europeo?

Su historia en nuestro país, si bien se puede considerar relativamente breve, es cuanto menos intensa, muy influenciada por el ámbito europeo. Elegir un punto de partida concreto resulta una tarea confusa, mas no es objetivo esencial de este presente trabajo.

Un primer hecho relevante puede ser considerado la creación, por parte del Consejo de Europa en 1967, de la «*Comisión Consultiva para estudiar las tecnologías y su potencial agresividad hacia los derechos de las personas*», de la que surgió la Resolución 509, de 1968, sobre «*Los Derechos Humanos y los nuevos logros científicos y técnicos*». Se empiezan a previsualizar las consecuencias negativas de la informática en la vida privada de las personas, preocupación constante para el Consejo a partir de ese momento. (Canales, 2007)

En consecuencia, según Canales, a finales de los años 70 se inician las primeras regulaciones nacionales sobre la protección de datos, aprobándose leyes en países como Alemania, Francia o Dinamarca. Mención especial merece el artículo 35 de la Constitución Portuguesa de 1976, que ya hablaba de la utilización de la informática y serviría como base al ya nombrado anteriormente artículo 18.4 de la Constitución Española (Maeztu, 2015): "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." El Parlamento Europeo también aprobará en 1979 la Resolución sobre «*La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática*». (Piñar, 2003)

Ya en los años 80, concretamente 1981, también Piñar (p.48):

“Desde el Consejo de Europa se dará un respaldo definitivo a la protección de la intimidad frente a la informática mediante el Convenio n.º 108, para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal. Este Convenio establece los principios y derechos que cualquier legislación estatal debe recoger a la hora de proteger los datos de carácter personal”.

Para Canales, (p.18) “al paso de los años, se ha convertido en el auténtico referente del derecho a la protección de datos personales tal y como hoy lo conocemos”. Este convenio, cuya entrada en vigor fue 1 de octubre de 1985 y España lo ratificó el 31 de enero de 1984, rezaba en su artículo 4 el compromiso de cada país a promover una legislación interna, (Pavón, 2001-2002) a lo más tardar la entrada en vigor de dicho convenio. (Convenio Nº108, 1981, art.4) Como costumbre, España se retrasaría e incumpliría durante varios años, hasta la llegada en 1992 de la LORTAD.

La LORTAD marcaría un hito histórico, al ser la primera normativa nacional aprobada en nuestro país. Nació con el propósito de desarrollar el artículo 18.4 de nuestra Constitución. Introdujo nuevos conceptos como la adecuación y calidad de los datos, la información en su recogida, el consentimiento del afectado, los datos especialmente protegidos (ideología, creencias...), la obligatoria seguridad de los datos o derechos como el de acceso, rectificación y cancelación. Además, introduce las sanciones económicas y encomienda el control de su aplicación a un órgano independiente, la Agencia de Protección de Datos (posteriormente Agencia Española de Protección de Datos). (Ley Orgánica Nº5, 1992)

Esta ley solo estaría en vigente durante un período de 7 años, debido a que en 1999 llegaría la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de

Carácter Personal (LOPD). Curiosamente es en 1999, meses antes, cuando la LORTAD se vio complementada por el Real Decreto 994/1999, de 11 de junio, que establecía el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, generando una situación confusa. En un inciso, mencionar que “la finalidad de un reglamento es facilitar la aplicación de la ley, detallándola y operando como instrumento idóneo para llevar a efecto su contenido”, (“ConceptoDefinición”, s.f) lo cual la LORTAD estuvo prácticamente toda su vida sin esta figura. Para Oltra (2017), “Una ley sin reglamento es como un jardín sin flores.”

La llegada de la LOPD estuvo directamente condicionada por la Directiva 95/46/CE del Consejo y el Parlamento Europeo de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Creó “un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea.” (“Eur-Lex”, s.f, a) En definitiva, esta directiva supuso una precisión y ampliación de los principios ya contenidos en el Convenio Nº108 de 1981. (Directiva 95/46/CE, 1995, Considerando 11)

No obstante, centrándonos en el motivo principal que propiciaría la derogación de la LORTAD y la llegada de la LOPD, lo encontramos en el Artículo 3 de dicho documento: “Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento **no automatizado** de datos personales contenidos o destinados a ser incluidos en un fichero”. La LORTAD solo hacía referencia al tratamiento automatizado (no incluía el soporte papel), lo cual hacía necesaria una reforma de nuestra legislación. La LOPD, además, aporta el derecho de oposición (completando así los llamados derechos ARCO, que posteriormente veremos con más detalle) e incluye la nueva definición “encargado del tratamiento de datos”, separándola del “responsable del fichero o tratamiento” únicamente visto en la LORTAD.

La LOPD, al igual que le pasara a su ley predecesora, tuvo que esperar bastantes años para verse complementada reglamentariamente. Así, la LOPD estuvo conviviendo con un reglamento “que no era suyo”, ya que originariamente pertenecía a la LORTAD, hasta que en 2007 se aprobara el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Básicamente, el propio reglamento señala que nace para “desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto grado de precisión que dote de seguridad jurídica al sistema”.

Realizando una parada en el curso de los acontecimientos, es conveniente recordar las preguntas formuladas en los inicios del apartado, desde cuándo la protección de datos de carácter personal es un derecho fundamental, tanto a nivel europeo como nacional. Resulta curioso que estos dos sucesos se dieran prácticamente paralelos en el tiempo, ambos en el año 2000.

En primer lugar, respecto al Derecho Comunitario Europeo, ocurre tras proclamarse en Niza la Carta de los Derechos Fundamentales de la Unión Europea, el 7 de diciembre. En ella, el artículo 8.1 reconoce que “toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”. (Carta de los derechos fundamentales de la Unión Europea, 2000) A diferencia de lo señalado en la antigua Resolución 509 o en el Convenio Nº108, ya no es un derecho dependiente de la informática o la intimidad, sino pasa a ser sustantivo y autónomo. (Canales, 2007)

En segundo lugar, concerniente a España, el hecho clave fue la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, “la que definitivamente ha reconocido que el derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un derecho autónomo e independiente”. (Piñar, 2003, p.51) La sentencia explica que, el derecho a la protección de datos va más allá de lo íntimo (aspecto ya protegido por el artículo 18.1), porque su objeto de protección es la totalidad de los datos personales. Una foto de una persona o su DNI no son datos íntimos, ni siquiera privados, pero son datos personales con la capacidad de identificar a un individuo, constituyendo una posible amenaza.

Tras el paréntesis, a modo de conclusión, es necesario puntualizar que la LOPD, y su posterior reglamento, no componen la última tendencia en materia de protección de datos. El Reglamento General de Protección de Datos se presenta como uno de los hitos históricos más importantes, sino el que más. Junto a él, la necesidad de readaptar nuevamente nuestra legislación interna, estando en proceso el Proyecto de Ley Orgánica de Protección de Datos. A ello dedicaremos el siguiente capítulo.

3 MARCO LEGAL

En el presente capítulo será objeto de análisis el nuevo Reglamento General de Protección de Datos, con especial atención a sus novedades y modificaciones incorporadas respecto a su anterior normativa europea, la Directiva 95/46, y española, la LOPD de 1999 y su reglamento de desarrollo de 2007. La lista de cambios es extensa, por lo que la legislación española tiene bastantes tareas por hacer. Ante este hecho, surge la nueva Ley Orgánica de Protección de Datos de Carácter Personal, con el objetivo de adecuarse al nuevo Reglamento europeo de mayo de 2018, pero que en julio sigue siendo un proyecto pendiente de aprobar.

3.1 REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

En un primer lugar, con el objetivo de facilitar la comprensión y evitar posibles confusiones en las próximas líneas, se realizarán dos precisiones referentes a términos jurídicos:

- Distinción entre los conceptos entrada en vigor y plena aplicación. Varias veces han sido nombrado ambos conceptos en páginas anteriores del presente trabajo, pudiendo parecer, en buena medida, sinónimos. No obstante, presentan distintas connotaciones. Una norma entra en vigor cuando puede comenzar a desplegar los efectos jurídicos para los que fue creada. La vigencia de una norma está vinculada a su publicidad, ya que es requisito obligatorio la publicación en un órgano oficial, normalmente el Boletín Oficial del Estado (BOE). Si no es establecida fecha alguna en su contenido, esta pasará a ser veinte días después de su publicación en el BOE. (Universitat de València, s.f) Por otro lado, plena aplicación hace referencia a la fecha en que la norma pasa a ser de obligado cumplimiento, iniciándose así su carácter sancionador.
- Reglamento en el ordenamiento jurídico español y Reglamento en el derecho comunitario europeo. El reglamento en el ordenamiento español fue tratado en el capítulo anterior, viéndose su valor subordinado a las leyes y con la finalidad de complementarlas. No obstante, los reglamentos lanzados por el Consejo y la Comisión Europea poseen un carácter mucho más fuerte que los anteriores, situándose incluso por encima de la Constitución Española. Obligatorio en todos sus elementos, son directamente aplicables en cada Estado miembro. ("Eur-

Lex”, s.f, b) Resulta conveniente también matizar la diferencia entre reglamentos y directivas europeas (recordemos la anteriormente vista Directiva 95/46/CE). Según la misma fuente, si bien los reglamentos son de por sí directamente aplicables, las directivas muestran el resultado que se ha de obtener, dejando cierta libertad a los Estados en cuanto a forma y medios de llegar al objetivo, quizás con la aprobación de una nueva ley orgánica o desarrollándola reglamentariamente.

3.1.1 CONSIDERACIONES INICIALES

Reglamento (Ue) 2016/679 Del Parlamento Europeo y Del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Con este título comenzaba el Diario Oficial de la Unión Europea (DOUE) L 119 del 4 de mayo de 2016, dando así a luz al ya citado Reglamento General de Protección de Datos, también conocido por sus siglas RGPD.

En él, 88 páginas, constituidas por 173 considerandos previos, junto a 99 artículos divididos en 11 capítulos. La RGPD deroga a la vigente, desde 1995, Directiva 95/46/CE.

En una materia marcada por la constante evolución, más de 20 años se apetecen demasiados. Es cierto, también, que ambas normativas no soportan verdaderamente comparación, debido a ser dos instrumentos del Derecho Comunitario Europeo distintos -vista ya sus diferencias-. Por consiguiente, no se debe caer en la confusión que la materia de protección de datos en ámbito europeo lleva tanto tiempo desactualizada, ya que la nombrada Directiva trajo consigo sucesivos cambios posteriores en la legislación interna de los Estados miembros. Precisamente, esta última apreciación, es una de las causas que ha propiciado el desarrollo del Reglamento, la disparidad legislativa entre países.

Pese al carácter reglamentario, es decir, su total e inmediata inclusión a la normativa interna de todos los Estados miembros, este hecho no provoca la derogación de las correspondientes leyes orgánicas vigentes, si bien se ven en parte desplazadas hasta su adaptación al RGPD. Esto ocurre debido a que, el Reglamento, deja en manos de legislaciones internas diversos aspectos y directrices (quizás demasiados), por ende, ambas normativas, europea y nacional, coexistirán. En España, este suceso deriva en una nueva Ley Orgánica de Protección de Datos -ya en proceso, será vista en apartados

posteriores-, donde se concretarán ciertos aspectos del RGPD y que sustituirá a la LOPD actual de 1999.

Un antes y un después en la breve historia de la protección de datos, el RGPD trae consigo, en palabras de Piñar (2016, p.14) “un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información”, en la búsqueda de una mayor proactividad y preocupación de las organizaciones por salvaguardar la integridad de los datos personales.

3.1.2 ETAPAS, JUSTIFICACIÓN Y OBJETIVOS

Resulta de sumo interés el hecho de su mayor actualidad en nuestro presente año, 2018, tras haber pasado ya dos años de la publicación en el DOUE. La respuesta se puede encontrar en el capítulo XI artículo 99 de la presente normativa, siendo, curiosamente, el primer artículo que hacemos referencia el último contemplado por dicho Reglamento:

Artículo 99

Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.
2. Será aplicable a partir del 25 de mayo de 2018.

L 119/88

ES

Diario Oficial de la Unión Europea

4.5.2016

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Figura 3.1. Artículo 99 RGPD

Fuente: Reglamento 2016/679 (2016, pp. 87-88)

Los máximos órganos europeos decidieron separar en dos años la fecha de entrada en vigor y la fecha de aplicación, quedando así un extenso período de dualidad legislativa, puesto que conviven la Directiva 95/46/CE, de plena aplicación, junto al RGPD, entrado en vigor, pero no a todos sus efectos. Se buscaba el objetivo de dotar de un buen margen a las organizaciones para “ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD”. (AEPD, 2017, p.2) Así, durante este período transitorio que finaliza el 25 de mayo de 2018, la LOPD y su Reglamento tienen plena vigencia en España, si bien las organizaciones poco a poco

deben ir adecuando sus actuaciones y políticas al nuevo RGPD, con el fin de llegar preparadas a la señalada fecha.

Una vez llegada la fecha, los responsables de las organizaciones deben asumir, también en palabras de la AEPD (2017, p.2):

“La norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite”.

Son muchos los conceptos, principios y mecanismos que el RGPD mantiene respecto a los establecidos por la Directiva 95/46 y por las normas nacionales que la aplican. Por ello, las organizaciones que en la actualidad cumplen adecuadamente con la LOPD española tienen una buena base de partida para evolucionar hacia una correcta aplicación del nuevo Reglamento, señala la AEPD.

Sin embargo, ya a finales de abril, el 25 de mayo es inminente y muchas organizaciones parecen haber descuidado este aspecto, o bien no están informados de su existencia o no saben cómo actuar. Pese a la citada similitud, existen una serie de cambios y nuevas obligaciones que deben ser objeto de un análisis detallado, no teniendo igual incidencia en todas las organizaciones. Además, muchos aspectos no disponen de una rápida implantación. En el próximo capítulo se analizarán varias empresas en vista de comprobar si han realizado sus correspondientes tareas en materia de protección de datos, especial interés en aquellas que disponen de recursos más limitados, las pymes.

Nuestro punto de partida ha sido situado el 4 de mayo de 2016, día en que el Diario Oficial de la Unión Europea publicó el Reglamento. No obstante, no cabe duda de que un documento de tales características y de una importancia difícil de cuantificar no surge y es redactado de la noche a la mañana. Piñar (2016, p.13) señala “Tras un largo y azaroso proceso de elaboración que dio comienzo formalmente el pasado día 25 de enero de 2012 (pero que desde mucho antes estaba ya gestándose), el Reglamento General de Protección de Datos ha sido publicado”.

El proceso de elaboración será visto más detalladamente gracias a la publicación en segundo trimestre de 2016 de Gabilex, revista del Gabinete Jurídico de Castilla-La Mancha, donde D. Roberto Mayor Gómez afrontó este tema de una manera correcta y ajustada a nuestro trabajo. (Mayor, 2016, pp.7-8)

Así, su origen desde el punto de vista institucional puede situarse en 2010 en el Programa de Estocolmo, donde el Consejo y la Comisión Europea evaluaron el

funcionamiento de los instrumentos de la Unión Europea en materia de protección de datos y vieron la posibilidad de presentar, en caso necesario, nuevas iniciativas.

Tras su resolución, el Parlamento Europeo vio positiva la elaboración de un régimen general de protección de datos. Por lo tanto, en el seno de la Unión Europea comienza a considerarse la necesidad de establecer un marco más sólido y coherente en materia de protección de datos en la UE, que evite la excesiva disparidad entre países y refuerce la seguridad jurídica tanto de los ciudadanos, como de los agentes económicos y autoridades públicas.

Comienza así una amplia consulta entre todos los actores interesados, plasmadas en la Resolución del Parlamento Europeo, de 6 de julio de 2011, donde queda aprobado un informe favorable a reformar el marco de la protección de datos. El Comité Económico y Social Europeo también se mostró favorable en la postura de garantizar una aplicación más coherente de las normas sobre este derecho fundamental y una revisión adecuada de la Directiva 95/46/CE.

Es a finales de enero de 2012 cuando se elabora por parte de la Comisión Europea la primera propuesta, el primer borrador de lo que hoy día conocemos como Reglamento General de Protección de Datos. Sometido a numerosas modificaciones durante más de 3 años, sería el 15 de diciembre de 2015 la fecha en que el Parlamento y el Consejo alcanzan el acuerdo sobre el texto, que meses más tarde fuera publicado en el DOUE.

Entre líneas, son varias las referencias ya hechas respecto a las causas y justificaciones que han motivado la redacción del presente RGPD. De igual manera e íntimamente relacionado, ocurre con los objetivos y retos que se pretenden alcanzar con su proclamación.

Las principales justificaciones son:

- La necesidad de reformar y actualizar la legislación vigente europea. La Directiva 95/46/CE, si bien nadie duda de su importancia y buen hacer, (basta con ver que RGPD mantiene gran parte de ella) data de 1995. Resulta tarea imposible realizar un listado de los cambios que se han dado desde entonces en las áreas de tecnologías e información, especialmente el crecimiento de Internet en todos sus ámbitos. En consecuencia, la Directiva se encontraba, en parte, obsoleta. El considerando 6 afirma: “La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa”. (Reglamento 2016/679, 2016)

- La disparidad existente entre las distintas legislaciones internas de los Estados miembros. Especialmente para las organizaciones con presencia en varios estados, resultaba difícil y fastidioso tener en cuenta la legislación vigente de cada país según actuara, pudiendo diferir bastante de cualquier otro. El considerando 7 muestra: “Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior”.
- “La definitiva consolidación de la protección de datos como derecho fundamental” (Piñar et al, 2016, p.16) único e independiente. El desarrollo del Reglamento confirma el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, el 7 de diciembre de 2000 en Niza. En ella, reconoce que “toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen”. Completa separación de conceptos como intimidad o informática.
- También en palabras de Piñar: “La extensión del ámbito territorial de aplicación de las normas protectoras”. Organizaciones extranjeras, aunque actuaran en Europa, no estaban regidas por la antigua normativa. El artículo 3.2 del Reglamento indica: “El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión”. En síntesis, cualquier empresa cual sea su procedencia, que venda o preste servicios en la UE, tendrá que cumplir el Reglamento. Esta mayor seguridad para el ciudadano era necesaria, ante un mercado prácticamente global.

En referencia a los objetivos, pueden ser nombrados:

- El refuerzo de los derechos del ciudadano, cada vez más expuesto al tratamiento de sus datos. Considerando 11: “La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal”. Derecho a la portabilidad o derecho al olvido se añaden a los ya conocidos derechos de acceso, rectificación, cancelación y oposición (ARCO).
- La obtención de mayores garantías de seguridad del ciudadano “por defecto”. Mediante nuevas obligaciones en la información y el consentimiento, las organizaciones deberán prestar mayor atención a si realmente están autorizados para tratar los datos de sus usuarios, además de aumentar la cantidad de

información que deben recibir. Estas medidas están respaldadas con un aumento considerable de las cifras de las sanciones.

- Nuevamente la cita de Piñar: “Nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información”. Se busca de las organizaciones que vayan más allá y no se limiten a cumplir las obligaciones, que muestren una responsabilidad proactiva y tengan siempre en mente la prevención de riesgos en sus tratamientos de datos personales, incluso en el momento inicial de diseño y creación del tratamiento. Análisis de riesgos, evaluaciones de impacto y la elección de un Delegado de Protección de Datos, siempre atendiendo a las circunstancias de cada empresa, son algunas de las medidas impuestas.
- Confirmar la importancia de las autoridades públicas independientes, en España la Agencia Española de Protección de Datos. Dentro del artículo 51 del presente RGPD: “Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento...”. Además de la supervisión, en páginas anteriores se hizo hincapié en que el Reglamento mantiene ciertos aspectos bajo legislación nacional, influencia directa con la AEPD. Asimismo, en el párrafo segundo del mismo artículo: “Las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII”. Las autoridades de los distintos Estados miembros colaborarán si fuese necesario, aspecto tratado con más detalle en el próximo apartado.

3.1.3 CONTENIDO PRINCIPAL Y NOVEDADES

En el presente apartado continuamos nuestro análisis del Reglamento General de Protección de Datos, en el cual serán tratadas sus principales novedades y modificaciones introducidas. No obstante, para su mejor comprensión, se harán referencias a conceptos, principios o derechos ya introducidos en la LOPD, legislación nacional aún vigente, con el fin de obtener un diagnóstico más amplio de la llegada de este Reglamento.

Primeramente, serán vistas una serie de definiciones, recogidas en el artículo 4, que se repetirán a lo largo del análisis: (Reglamento 2016/679, 2016)

- **Datos personales:** “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación [...] o uno o varios elementos propios de la identidad física,

fisiológica, genética, psíquica, económica, cultural o social de dicha persona”. El interesado sería, por tanto, la persona objeto del tratamiento de sus datos personales.

- **Tratamiento:** “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión”.
- **Responsable del tratamiento:** “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento”.
- **Encargado del tratamiento:** “la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”. Responsable y encargado están fuertemente relacionados, pero poseen obligaciones ciertamente distintas. Su relación debe ser contractual.

A modo de ilustración, es presentado en formato tabla los distintos elementos que forman el conjunto de novedades a estudiar, junto a sus correspondientes artículos y considerandos. Acto seguido, serán comentados cada uno de ellos. Para mayor grado de detalle, se facilita y recomienda su revisión íntegra en el Reglamento. *Enlace al Reglamento 2016/679 formato .pdf*

| Novedad | Localización |
|--|--------------------------------------|
| Ámbito territorial | Considerandos 22-24. Art. 3 |
| Principios relativos al tratamiento | Considerando 39. Art. 5.1 |
| Condiciones para el consentimiento | Considerando 32. Art. 7 |
| Consentimiento del menor | Considerando 38. Art. 8 |
| Nuevas categorías especiales de datos | Considerandos 51-54. Art. 9 |
| Transparencia e información a los interesados | Considerandos 39; 58-62. Arts. 12-14 |
| Nuevos derechos: olvido, portabilidad y limitación | Considerandos 65-68. Arts. 17-20 |
| El principio de responsabilidad proactiva | Considerando 74. Arts. 5.2; 24 |

| Novedad | Localización |
|--|------------------------------------|
| Privacidad desde el diseño y por defecto | Considerando 78. Art. 25 |
| Relaciones responsable-encargado | Considerando 81. Art. 28 |
| Registro de las actividades de tratamiento | Considerando 82. Art. 30 |
| Notificación violación de seguridad a la AEPD | Considerandos 85-88. Art. 33 |
| Evaluación de impacto de protección de datos | Considerando 84. Arts. 35-36 |
| Delegado de protección de datos | Considerando 97. Arts. 37-39 |
| Transferencias internacionales | Considerandos 101-114. Arts. 44-47 |
| Cooperación entre autoridades y ventanilla única | Considerando 127. Arts. 60-63 |
| Indemnización y sanciones | Considerandos 146-152. Arts. 82-84 |

Tabla 3-1. Novedades y sus artículos

Fuente: elaboración propia/ a partir de Reglamento 2016/679 (2016)

1. **Ámbito territorial.** Todas las empresas establecidas en la Unión Europea están acogidas al Reglamento, independientemente de que los tratamientos de datos que realicen tengan o no lugar en la Unión.

El aspecto más novedoso trata sobre las empresas establecidas fuera del territorio europeo. Exentas anteriormente de cualquier responsabilidad, el presente Reglamento amplía su ámbito de aplicación a estas organizaciones en los siguientes casos:

- Empresas que oferten bienes o servicios a personas físicas que se encuentren en la Unión Europea, independientemente de que medie pago. Desde Facebook, empresa de servicios gratuita, hasta Amazon, empresa principalmente de comercio electrónico, se regirán a partir de ahora por el RGPD en sus actividades en territorio europeo. Sin embargo, cabe preguntarse cuándo se considera ofrecimiento de bienes y servicios. El considerando 22 señala: “debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros [...] la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, no basta para determinar dicha intención”. Serán válidos factores como el idioma o la moneda utilizadas para la transacción, así como la mención a clientes y usuarios que se encuentren

en la UE. Por lo tanto, aunque sea posible acceder a una página web de origen chino y comprar un smartphone, esta no tiene que estar necesariamente regida por el RGPD.

- Empresas cuyas actividades de tratamiento estén relacionadas con la observación o control del comportamiento de individuos en la Unión, siempre que este comportamiento tenga lugar en la UE. El considerando 24, igualmente: “debe evaluarse si las personas físicas son objeto de un seguimiento en internet [...] elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes”.

2. Principios relativos al tratamiento. En el artículo 5.1.a se menciona el principio de licitud, lealtad y transparencia: “Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado”. Mantiene una fuerte relación con el artículo 4.7 de la LOPD: “Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos”. Respecto a la transparencia, aspecto que el RGPD le da un papel fundamental, la desarrolla en su artículo 12.

Principio de integridad y confidencialidad, artículo 5.1.f: “se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas”. Si bien guarda estrecha relación con el artículo 9 de la LOPD titulado Seguridad de los datos, las modificaciones en materia de seguridad son muy importantes en el RGPD. La LOPD contenía una previsión genérica sobre la seguridad de los datos, estableciendo unas condiciones concretas que serían desarrolladas por su reglamento del año 2007: “No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos”. (Ley Orgánica Nº15, 1999, art. 9)

Así, en dicho Reglamento, más de 35 artículos detallarían las medidas de seguridad obligatorias para las organizaciones, distinguiendo entre modos de tratamiento y niveles de seguridad según la tipología de los datos personales. Con la llegada del RGPD, se reemplaza este sistema cerrado por uno más abierto, basado en la responsabilidad proactiva y un enfoque de riesgo constante. Las empresas deberán, por sí mismas, analizar qué datos tratan y los tratamientos que le aplican, con el fin de encontrar las medidas apropiadas a sus circunstancias que garanticen la integridad y confidencialidad. (San José, 2018) La AEPD (2017, p.4) ejemplifica:

“Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles”.

3. Condiciones para el consentimiento, consentimiento del menor y transparencia e información a los interesados serán enlazados y analizados en el próximo subapartado, dada su relevancia y número de modificaciones.

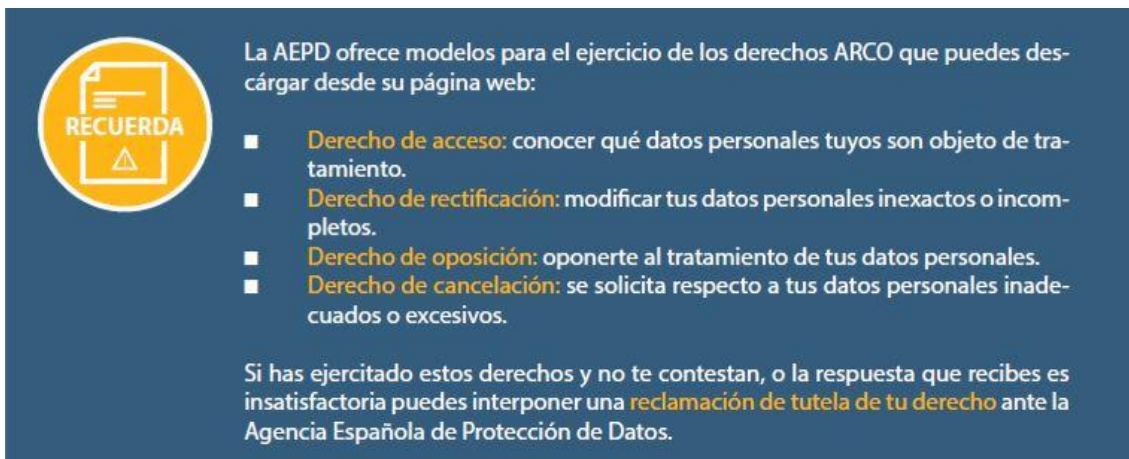
4. Nuevas categorías especiales de datos. Definidos en el Considerando 51: “datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos”. Son datos que requieren una mayor protección, estando salvo excepciones prohibido su tratamiento.

Origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, vida sexual y datos relativos a la salud son tipologías de datos ya contemplados en la LOPD, a los que el RGPD añade los datos genéticos y datos biométricos -definidos en el artículo 4.13 y 4.14, respectivamente- y los relativos a las orientaciones sexuales de una persona física, ampliando el concepto de vida sexual.

Algunas de las excepciones que permiten su tratamiento, recogidas en el artículo 9, son el consentimiento explícito del interesado para las finalidades especificadas, la protección de intereses vitales del interesado, datos que el interesado haya hecho públicos o datos de interés público en el ámbito de la salud pública, investigación científica o histórica y fines estadísticos.

En cuanto a las medidas para asegurar su mayor protección, las organizaciones que traten estos datos estarán obligadas, por norma general, a realizar un registro de las actividades de tratamiento y una evaluación de impacto, conceptos luego vistos.

5. Derecho al olvido, derecho a la portabilidad y derecho a la limitación del tratamiento. Tres nuevos derechos incorporados a disposición de los individuos, si bien los dos primeros guardan fuerte relación con parte de los ya conocidos derechos ARCO.



La AEPD ofrece modelos para el ejercicio de los derechos ARCO que puedes descargar desde su página web:

- **Derecho de acceso:** conocer qué datos personales tuyos son objeto de tratamiento.
- **Derecho de rectificación:** modificar tus datos personales inexactos o incompletos.
- **Derecho de oposición:** oponerte al tratamiento de tus datos personales.
- **Derecho de cancelación:** se solicita respecto a tus datos personales inadecuados o excesivos.

Si has ejercitado estos derechos y no te contestan, o la respuesta que recibes es insatisfactoria puedes interponer una **reclamación de tutela de tu derecho** ante la Agencia Española de Protección de Datos.

Figura 3.2. Derechos ARCO según AEPD

Fuente: AEPD (2017b, p.22)

La Agencia Española de Protección de Datos muestra en su publicación *Guía para el Ciudadano* (AEPD, 2017b) información sobre todos los derechos contemplados en el RGPD y cómo ejercerlos, todo en un lenguaje claro y con numerosos ejemplos y gráficos. *Acceso a la guía*

El derecho de supresión o derecho al olvido. Consiste en aplicar los derechos de cancelación y oposición a los buscadores online (Google, Yahoo...) para impedir la difusión de la información cuando ésta es obsoleta o no tiene relevancia ni interés público. La información no aparecerá en los resultados de búsquedas, pero esto no significa que sea borrado de la fuente original. (AEPD, 2017b) Es un derecho no exento de polémica, pues cabe la posibilidad de considerarlo una forma de censura, por ejemplo, para borrar rastros de casos de corrupción o deudas. Para un uso más adecuado, cada caso se trata por separado. Los principales buscadores han habilitado formularios para facilitar su ejercicio, como es el caso de Google, muy informativo y claro en su lenguaje. (Google, s.f) *Enlace al formulario*. En caso de obtener una denegación en la solicitud, es posible reclamar a la AEPD que intervenga.

El Reglamento, en su artículo 17, trata más ampliamente este derecho y lo traslada a cualquier responsable del tratamiento, contemplando tanto circunstancias en la que es válida su aplicación como situaciones en las que prevalecen otros intereses.

El derecho a la portabilidad, artículo 20 del RGPD. Supone una ampliación del derecho de acceso. El interesado, al obtener por parte del responsable la información referente a sus datos personales y estado del tratamiento, esta debe ser proporcionada en un formato estructurado, de uso común y lectura mecánica, permitiendo la transmisión de un responsable a otro sin que el primero pueda oponerse.

Este derecho podrá aplicarse si el tratamiento es por medios automatizados y está basado en el consentimiento o en un contrato. La transferencia entre responsables se dará si es técnicamente posible.

Derecho a la limitación del tratamiento. En el artículo 4.3 del RGPD se define limitación del tratamiento: “el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro”. Es síntesis, datos que existen, por motivos legales u otros, y que el interesado puede bloquear durante un período su tratamiento, limitando al responsable exclusivamente a su mera conservación (salvo excepciones como que cambie de idea y preste consentimiento, para ejercicio o defensa de reclamaciones o datos que sean de interés público).

El interesado puede hacer uso de este derecho, entre otras situaciones, mientras espera el resultado de una impugnación hecha al responsable por inexactitud de los datos, o cuando el responsable ya no necesitara los datos para los fines establecidos pero el interesado los necesitara para ejercicio o defensa de reclamaciones.

6. Principio de responsabilidad proactiva. Eje central del nuevo RGPD, tanto por significado e importancia como por el resto de medidas que surgen de sí mismo. El responsable, teniendo en cuenta la naturaleza, el contexto y los fines del tratamiento, así como los riesgos y gravedades de los derechos y libertades de las personas, aplicará medidas oportunas y eficaces que garanticen el cumplimiento del Reglamento, además de poder demostrar este cumplimiento ante interesados y autoridades. (Reglamento 2016/679, 2016)

En términos prácticos, comenta AEPD (2017a) este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. Una vez generado el conocimiento, determinarán explícitamente y de manera demostrable, las medidas y formas de actuar que mejor se adecuen a la organización en su tarea de cumplir con el RGPD. Por tanto, exige una actitud consciente y proactiva por parte de las organizaciones, especialmente ante el riesgo de los derechos y libertades de los ciudadanos.

Varias medidas que se desprenden de este principio son el registro de actividades de tratamiento, la privacidad desde el diseño y por defecto, notificaciones de violaciones de seguridad, evaluación de impacto o la figura del Delegado de Protección de Datos.

7. Privacidad desde el diseño y por defecto. Constituyen el principal estandarte de la responsabilidad proactiva. El responsable debe pensar en términos de protección de datos durante todo el transcurso del tratamiento, inclusive el momento de diseño o creación, es decir, con anterioridad al inicio del tratamiento. (AEPD, 2017a)

La privacidad desde el diseño, según el considerando 78 del RGPD, supone que, durante el desarrollo, diseño y uso de aplicaciones, servicios y productos basados en el tratamiento de datos, se tengan en cuenta en todo momento el cumplimiento de las garantías del Reglamento. Este concepto pretende terminar con el hecho de primero desarrollar el producto y posteriormente tratar los aspectos privados y legales.

Respecto a la privacidad por defecto, en el artículo 25.2: “por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y [...] datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas”. Un ejemplo de mala práctica de este concepto es el exceso de permisos solicitados por una aplicación en nuestro teléfono (un juego que solicita acceso a los SMS). Por otro lado, una buena práctica se daría si tras el registro en una red social, esta activara por defecto una configuración alta de privacidad, por ejemplo, prohibiendo ver el perfil a usuarios no agregados como amigo.

8. Relaciones responsable-encargado. El responsable “elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento”, dicta el artículo 28. Este mismo caso se aplica si el encargado subcontractara operaciones a otro encargado.

Las relaciones entre responsable y encargado deben formalizarse en un contrato por escrito, estableciendo el objeto, duración y finalidad del tratamiento, el tipo de datos personales y las obligaciones y derechos del responsable. Además, se pactará la obligación del encargado a actuar siempre bajo instrucciones del responsable, o a prestar colaboración al responsable si fuese necesario demostrar el cumplimiento de las obligaciones. Los contratos concluidos con anterioridad a la aplicación del RGPD en mayo, deben modificarse y adaptarse para respetar este contenido. (AEPD, 2017a)

La figura del encargado ha ganado protagonismo con la llegada del Reglamento. Si bien la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, existen obligaciones expresamente dirigidas a los encargados, aspecto innovador frente a la anterior Directiva 95/46 y leyes nacionales, según también AEPD. Algunas de las obligaciones, atendiendo a las circunstancias del tratamiento y sensibilidad de los datos, pueden ser el registro de actividades del tratamiento o la designación de un Delegado de Protección de Datos.

9. Registro de las actividades de tratamiento. Uno de los aspectos clave de la LOPD resulta la obligación de notificar a la AEPD de la creación de ficheros de datos personales y registrarlos en su base de datos. Sin embargo, el 25 de mayo, plena aplicación del RGPD, esta obligación desaparece al no contemplarla el Reglamento. El RGPD introduce el registro de las actividades de tratamiento, un registro en sintonía con la responsabilidad proactiva, pues su función básica es demostrar el cumplimiento de las medidas. Además, al contrario que el establecido en la LOPD, se ajusta a las características de las empresas, no siendo obligatorio su realización para todas ellas.

Así, las empresas con menos de 250 trabajadores están exentas, salvo aquellas que los tratamientos que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados y sean constantes en el tiempo, o incluyan categorías especiales de datos o datos relativos a condenas e infracciones penales. (AEPD, 2017a)

En cuanto a las empresas que estén obligadas, el registro lo harán tanto responsables como encargados, por escrito y a entregar a la AEPD. En él se detallará, entre otros aspectos, nombre y datos del responsable/encargado, finalidades del tratamiento, plazo previsto para supresión de los datos o descripción de las medidas de seguridad.

10. Notificación violación de seguridad a la AEPD. El artículo 4 muestra la confusa definición de violación de seguridad de los datos personales: “ocasiona la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”. AEPD da ejemplos tales como pérdida de un ordenador portátil, acceso no autorizado a bases de datos de la empresa o borrado accidental de algún fichero de datos.

El artículo 33 contempla la obligación de las empresas a notificar estas violaciones de seguridad a la autoridad de control competente (AEPD en nuestro caso) a menos que sea improbable que dicha violación constituya un riesgo para los derechos y las libertades de las personas, y a ser posible en un plazo de 72 horas, teniendo que justificar los motivos de la dilación si se supera ese tiempo límite. La notificación deberá ser informada igualmente a los interesados afectados, objeto de estudio del siguiente subapartado.

La notificación debe contener, como mínimo, la naturaleza de la violación, categorías y número aproximado de datos e interesados afectados, forma de contactar con el delegado de protección de datos u otro punto de información, describir las posibles consecuencias y medidas tomadas para poner remedio a la violación y sus efectos negativos.

11. Evaluación de impacto relativa a la protección de datos (EIPD). Deberá realizarse, por parte de los responsables del tratamiento, cuando sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas. Tratamientos a gran escala de datos sensibles y observación sistemática a gran escala de una zona de acceso público, son supuestos considerados por la AEPD (2017a).

El contenido mínimo, recogido en el artículo 35, trata sobre la descripción de las operaciones y fines del tratamiento, evaluación de la necesidad y proporcionalidad respecto a su finalidad y evaluación de los riesgos para las personas y medidas previstas para afrontarlos. Según artículo 36, si tras su realización los resultados de la EIPD muestran un alto riesgo que el responsable no pueda hacer frente, este consultará a la autoridad de control antes de iniciar el tratamiento, siendo asesorado en un plazo de ocho semanas, prorrogable seis semanas más según complejidad.

El RGPD prevé que las evaluaciones de impacto se lleven a cabo antes de empezar el tratamiento, lo cual el Reglamento no se extiende a las operaciones que ya estén en curso en la fecha de aplicación, salvo que se produzcan posteriormente cambios en los riesgos relativos al tratamiento. Ejemplos de cambios pueden ser la aplicación de nuevas tecnologías a ese tratamiento, la recogida de más datos o finalidades del tratamiento distintas a las acordadas en su momento. (AEPD, 2018)

12. Delegado de protección de datos (DPD). Figura con cualidades profesionales, especialmente conocimientos del Derecho y la práctica en materia de protección de datos, que será de obligatorio nombramiento para ciertas organizaciones, con el fin de supervisar el cumplimiento del RGPD entre otras funciones.

El DPD deberá ser nombrado en autoridades y organismos públicos. Respecto al sector privado, será en empresas responsables o encargadas de tratamientos de datos que, a gran escala, requieran una observación habitual y sistemática de interesados o utilicen datos personales de categoría especial. El RGPD, así, no deja excesivamente claro qué empresas deberán nombrar esta figura, pues el término gran escala resulta difuso, siendo necesaria la intervención de la AEPD o la nueva LOPD.

Sus principales funciones están recogidas en el artículo 39, tales como informar y asesorar al responsable/encargado y empleados en materia de protección de datos, supervisar el cumplimiento de lo dispuesto en el RGPD y cooperar tanto con la autoridad de control (AEPD) como con los interesados en cuestiones relativas al tratamiento de sus datos personales.

El delegado podrá ser un trabajador que forme parte de la plantilla de la empresa responsable o encargada, o bien ser contratado de manera externa. El Reglamento,

además, contempla la posibilidad de nombrar un único DPD para un grupo empresarial, siempre que sea fácilmente accesible desde cada establecimiento

En cualquier caso, sus funciones requieren de total autonomía, no siguiendo órdenes de responsable o encargado, y su nombramiento y datos de contacto han de ser publicados y comunicados a la autoridad de control. Pese a no necesitar una titulación específica para ejercer el cargo, los conocimientos jurídicos en la materia son sin duda necesarios. Así, la AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos como herramienta útil a la hora de evaluar y facilitar la selección del candidato.

13. Transferencias internacionales. El artículo 33 de la LOPD dicta: “No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal [...] a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que [...] se obtenga autorización previa del Director de la Agencia de Protección de Datos”. El artículo 34 de la misma recoge una serie de excepciones por las cuales no haría falta la autorización de la AEPD (convenio del país con España, consentimiento del afectado, salvaguarda de un interés público...). Pese a ello, el RGPD actualiza y adecua esta materia a nuestro tiempo, donde las transferencias internacionales son fundamentales en el progreso y precisan de un sistema más amplio y permisivo.

Una importante novedad que incorpora el Reglamento es la posibilidad de que tanto responsable como encargado del tratamiento podrán exportar los datos personales. Se elimina la barrera impuesta por algunos Estados Miembros en los que el exportador debía ser siempre el responsable. Sin embargo, el cambio más significativo es el requisito de autorización administrativa (AEPD) a casos excepcionales, que pasa de norma general a ser una excepción muy aislada. (Noguer, 2018)

La Comisión Europea pasa a tener un papel relevante, siendo lícitas las transferencias a países que este organismo ha decidido que garantizan un nivel de protección adecuado, sin ningún tipo de autorización.

No obstante, en determinados casos, incluidos los previstos en el artículo 34 de la LOPD, también es posible la realización de transferencias sin necesidad de autorización a países no contemplados por la Comisión. Para ello, son necesarias una serie de garantías, recogidas en el artículo 46.2 del RGPD, y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. En este punto también se encuentran las normas corporativas vinculantes, que hacen referencia a los grupos empresariales y la transferencia de datos entre las empresas pertenecientes, regulado en el artículo 47.

14. Cooperación entre autoridades y ventanilla única. El sistema de ventanilla única permite a las empresas establecidas en varios Estados miembros o bien, estando presente en uno solo, hagan tratamientos que afecten significativamente a ciudadanos de varios Estados, tener a una única autoridad de protección de datos como interlocutora, (Mayor, 2016) llamada la autoridad de control principal. Es decir, una empresa española con filial en Francia, esta filial estará también bajo mandato de la Agencia Española de Protección de Datos. Desde el punto de vista del interesado, si este denunciara a la filial, deberá acudir a la autoridad francesa, la cual notificaría en cualquier caso a la AEPD.

Esta medida va en consonancia con objetivos propuestos por el Reglamento, como son el reducir las dificultades por diferencias legislativas que se le presentan a este tipo de empresas, y la cooperación entre las autoridades de control.

Así, según Mayor (2016) cada autoridad de protección de datos europea, al analizar una denuncia o autorizar un tratamiento, valorará si el supuesto tiene carácter transfronterizo, iniciando un procedimiento de cooperación entre las autoridades afectadas en caso afirmativo. El considerando 127, junto los artículos 60, 61, 62, contienen la extensa normativa acerca de esta materia, que contempla diversidad de situaciones y modos de actuación a seguir por parte de las autoridades de control.

15. Indemnización y sanciones. El RGPD presenta importantes modificaciones en el régimen sancionador, pasando a ser un sistema más flexible, gravoso para las organizaciones y viable para los interesados.

El artículo 82 del RGPD muestra: “Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización”. No obstante, este punto no resulta de absoluta novedad, pues la LOPD ya prevé en su artículo 19 el derecho a la indemnización. Las verdaderas modificaciones llegan en su procedimiento, complejo y lento para los interesados, pues son llevados a los tribunales y no gestionados en su totalidad por la AEPD. El RGPD pretende darle a esta previsión una mayor presencia, dotándola de una mayor sencillez y permitiendo al interesado ejercitar su derecho a través de un mandato a una organización o entidad pertinente, para que actúe en su nombre en todo el proceso de la reclamación. (Vázquez y de Miguel, 2017)

Otra novedad, recogida en el artículo 83: “cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos”, llevadas a cabo por la autoridad de control. Sin

embargo, no parece probable que los Estados miembros vayan a permitir que sus propios organismos públicos sean sancionados. (Vázquez y de Miguel, 2017)

Las principales modificaciones en el régimen sancionador corresponden a las cifras de las sanciones, siendo aumentadas por el RGPD considerablemente en busca de un mayor cumplimiento y concienciación de las empresas en materia de protección de datos. Las multas pasan a ser más cuantiosas y flexibles, basándose en algunos casos en el volumen de facturación anual.

La LOPD dispone de un sistema cerrado, con tres categorías de infracciones bien diferenciadas en las que quedan recogidos los distintos casos de incumplimiento de la norma, y cada una con sus cifras de sanción prefijadas.

La RGPD presenta un modelo más individualizado, donde las multas se impondrán en función de las circunstancias de cada caso, tales como naturaleza, gravedad y duración de la infracción, intencionalidad o negligencia, categoría de datos afectados y más recogidas en artículo 83.2. Las cifras aumentan considerablemente respecto a la LOPD, presentándose en el ámbito de las empresas dos posibles cuantías de referencia, una fijada máxima o una equivalente a su volumen de negocio total anual del ejercicio financiero anterior, optándose por la de mayor cuantía.

| | Leve | Grave | Muy grave |
|------|--|--|--|
| LOPD | 900€ - 40.000€ | 40.001€ - 300.000€ | 300.001€ - 600.000€ |
| RGPD | Sin cifra mínima Máxima 10 Millones € | Máxima de 10 millones € o 2% del volumen de negocio | Máxima de 20 millones € o 4% del volumen de negocio |

Tabla 3-2. Tipos de sanciones y cuantías en LOPD y RGPD

Fuente: Elaboración propia a partir de Vázquez y de Miguel (2017, p.8)

Además del radical aumento de las cifras, se han realizado modificaciones en las categorías, es decir, infracciones que en la LOPD se consideraban graves y pasan a ser muy graves en el RGPD. Algunos ejemplos son el tratamiento de datos con un consentimiento no válido y la obstaculización al interesado de los derechos ARCO, los cuales resultaban penados con un máximo de 300.000€ y ahora puede llegar a 20.000.000€ o más.

3.1.4 REFUERZO DE LA TRANSPARENCIA Y EL CONSENTIMIENTO

Un principio fundamental ya recogido en la Directiva 95/46 y que el RGPD reproduce, es la necesidad de una base que legitime el tratamiento de datos, es decir, una razón o motivo que lo haga válido. (AEPD, 2017a) En la RGPD estas bases se detallan en el

artículo 6.1, licitud del tratamiento: consentimiento, relación contractual, intereses vitales del interesado o de otras personas, obligación legal para el responsable, interés público o ejercicio de poderes públicos, e intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

El consentimiento del interesado no es, por tanto, la única razón legal para que exista un tratamiento de datos. Sin embargo, especialmente en las relaciones empresa y cliente o usuario, es la base legítima más utilizada, y la cual necesitaba una profunda renovación con vistas a la protección de los individuos.

El RGPD pretende acabar con el consentimiento tácito, sobreentendido o forzado, el cual muchas veces el interesado acepta sin ni siquiera saberlo. Para ello, se incorpora el necesario requisito de que el interesado muestre una acción positiva que manifieste el consentimiento, ya sea una declaración verbal, una firma electrónica o marcar una casilla en una página web. Fundamental es que esta declaración de consentimiento realizada por la empresa sea transparente, es decir, legible para todo tipo de usuarios, separada de las condiciones de uso y demás aspectos legales de la empresa y fraccionada, teniendo cada fin del tratamiento su correspondiente aceptación del consentimiento y no una que valga para todos. (Reglamento 2016/679, 2016)

El obligado acto afirmativo por parte del interesado va en sintonía con el principio de responsabilidad proactiva incluido en este Reglamento, donde la empresa debe estar preparada en todo momento para demostrar el cumplimiento de las obligaciones. Así, consentimientos basados en el silencio, casillas ya marcadas o la inacción no resultan válidos, según marca el considerando 32 del RGPD.

El consentimiento toma especial relevancia en los menores de edad. El RGPD marca en su artículo 8 los 16 años como edad mínima para que el tratamiento sea lícito. Si el niño es menor, será necesario el consentimiento de los padres o tutores legales. El Reglamento dicta a los responsables del tratamiento, en artículo 8.2, que realicen esfuerzos razonables para verificar que en dicho proceso intervienen los padres.

Pese a los 16 años que fija el RGPD, en el segundo párrafo del artículo 8.1 se hace referencia: “los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años”. España tiene marcado este límite de edad en los 14 años, contemplado en el Reglamento de desarrollo de la LOPD. (Real Decreto 1720/2007, 2007, art.13.1) No obstante, en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, la nueva LOPD próxima a entrar en vigor, la edad baja hasta el mínimo de los 13 años.

Es preciso recalcar que este proceso de renovación en los consentimientos no deroga a todos los anteriormente conseguidos, teniendo que solicitarlo de nuevo. Si la empresa, con anterioridad a mayo de 2018, ya había recibido por parte del cliente o usuario un consentimiento válido y acorde a lo exigido en el Reglamento, y siempre que lo pueda demostrar acorde al principio de responsabilidad proactiva, no tendrá obligación de realizar de nuevo el proceso.

Se trata de un aspecto no libre de confusiones e interpretaciones, pues muchas empresas pueden no estar completamente seguras o no recordar si el consentimiento tomado con anterioridad cumple las exigencias del presente. A efectos de asegurar el correcto cumplimiento del RGPD y evitar sus altas sanciones, buena parte de ellas han optado por renovar sus consentimientos, principalmente vía e-mail.

Esta propuesta de un consentimiento más claro y seguro para los individuos mantiene una fuerte relación con el principio de transparencia introducido en el artículo 5.1.a y ampliado en los artículos 12, 13 y 14 del Reglamento. El RGPD incorpora importantes novedades en la transparencia y la información que deben suministrar las organizaciones a sus interesados una vez comience el tratamiento de datos. La AEPD también materializó una guía centrada en esta materia en la cual nos basaremos, *Guía para el cumplimiento del deber de informar*. (AEPD, 2017c) [Enlace a la guía](#)

Según el considerando 58 del RGPD: “toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo”. Por tanto, la información siempre deberá darse por escrito y se evitarán las fórmulas especialmente farragosas y que incorporan remisiones a los textos legales, no comprendidos por gran parte de las personas. (AEPD, 2017a)

La lista de elementos que deben ser objeto de información ha aumentado respecto a la LOPD. A los ya incluidos en esta ley, se añaden los datos de contacto del delegado de protección de datos -si lo hubiera-, la base legítima del tratamiento -consentimiento entre ellas, recordar las primeras líneas de este subapartado-, el plazo de conservación de los datos, la existencia de procesos automatizados o elaboración de perfiles, la previsión de transferencias a terceros países y el derecho a presentar una reclamación ante las autoridades de control. Si ocurre el caso que los datos no sean recabados por el propio individuo, por ejemplo, una cesión legítima, se informará del origen y las categorías de los datos en un plazo máximo de un mes. (AEPD, 2017c)

Un aspecto novedoso incorporado por el RGPD es la información por capas. Con el objetivo de facilitar a los responsables la tarea de informar y agilizar a los usuarios su comprensión, la información se dispondrá en dos niveles, una primera información básica y resumida en el mismo momento de la recogida de datos, y un enlace a la

segunda información adicional donde se detallarán el resto de informaciones en un formato más adecuado. Ambas pueden agruparse en epígrafes (AEPD, 2017c)

| Epígrafe | Información básica (1ª capa, resumida) | Información adicional (2ª capa, detallada) |
|--|--|---|
| “Responsable” (del tratamiento) | Identidad del Responsable del Tratamiento | Datos de contacto del Responsable |
| | | Identidad y datos de contacto del representante |
| | | Datos de contacto del Delegado de Protección de Datos |
| “Finalidad” (del tratamiento) | Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles | Descripción ampliada de los fines del tratamiento |
| | | Plazos o criterios de conservación de los datos |
| | | Decisiones automatizadas, perfiles y lógica aplicada |
| “Legitimación” (del tratamiento) | Base jurídica del tratamiento | Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. |
| | | Obligación o no de facilitar datos y consecuencias de no hacerlo |
| “Destinatarios” (de cesiones o transferencias) | Previsión o no de Cesiones | Destinatarios o categorías de destinatarios |
| | Previsión de Transferencias, o no, a terceros países | Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables |
| “Derechos” (de las personas interesadas) | Referencia al ejercicio de derechos. | Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento |
| | | Derecho a retirar el consentimiento prestado |
| | | Derecho a reclamar ante la Autoridad de Control |
| “Procedencia” (de los datos) | Fuente de los datos (cuando no proceden del interesado) | Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público |
| | | Categorías de datos que se traten |

Figura 3.3. Información por capas

Fuente: AEPD (2017c, p.5)

Además, de la misma manera que se obliga la notificación a la autoridad de control de las violaciones de seguridad, vista en el subapartado anterior, los interesados también recibirán esta información lo más rápido posible cuando suponga un alto riesgo para sus datos personales, salvo excepciones contempladas en el artículo 34.3.

3.2 PROYECTO DE NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

En el presente apartado será objeto de análisis la nueva legislación nacional en materia de protección de datos, que sustituirá a la LOPD de 1999. La principal justificación de esta ley es la adaptación al nuevo Reglamento europeo, el cual deja a discrecionalidad de los Estados miembros multitud de puntos importantes de su normativa que la antigua LOPD no contempla.

3.2.1 ETAPAS Y SITUACIÓN ACTUAL

La nueva ley tenía prevista su entrada en vigor en mayo de 2018, para así complementar correctamente al RGPD. Sin embargo, el 25 de mayo ya ha pasado y la ley aún está en pleno proceso parlamentario, iniciándose así un período de cierta inseguridad jurídica que todo parece indicar continuará hasta 2019.

El pasado 10 de noviembre de 2017 el Consejo de Ministros aprobó el primer Anteproyecto de Ley Orgánica de Protección de Datos, impulsado el 23 de junio de ese mismo año por el ministro de Justicia. Un Anteproyecto que se convertiría en el actual Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, el cual el 14 de noviembre empezaría su tramitación parlamentaria. (Barbarà, 2018) Comienza así una etapa de debate en el Congreso de los Diputados, donde los grupos políticos presentan sus puntos de vista y disconformidades respecto al Proyecto de ley presentado, principalmente a través de las enmiendas.

“Se denomina enmienda, en Derecho, a una propuesta de modificación de algún documento oficial, especialmente en los artículos y textos de leyes y proyectos de ley”. (Enmienda (ley), s.f) Así, hasta un total de 369 enmiendas fueron presentadas en el Congreso el 18 de abril, las cuales pueden ser revisadas en la web del Congreso y nos da una idea de lo lento que puede y va a llegar a ser el acuerdo y aprobación de esta nueva ley orgánica. (Enmiendas e índice de enmiendas al articulado ley nº121/000013, 2018)

3.2.2 DIFERENCIAS Y ADAPTACIÓN AL NUEVO RGPD/LOPD

El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, publicado el 24 de noviembre de 2017 en el Boletín Oficial de las Cortes Generales, contiene, exposición de motivos y disposiciones aparte, 78 artículos divididos en 9 capítulos. (Proyecto de Ley Orgánica nº121/000013, 2017)

En su primer artículo plasma su objeto, que no es otro que “adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 [...] y completar sus disposiciones·”.

Pronto, en el artículo 3, encontramos una de las principales novedades incorporadas, los datos referentes a personas fallecidas. Se contempla el poder de los herederos o personas designadas por el fallecido para “dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión”, salvo que el fallecido lo hubiese prohibido o lo establezca la ley. También se nombran aspectos que serán establecidos mediante real decreto -reglamento de desarrollo-, para el que seguro queda bastantes años.

Respecto al consentimiento, la nueva LOPD elimina el consentimiento tácito y se exige una manifestación de voluntad libre, específica, informada e inequívoca mediante una acción afirmativa, al igual que dictara el RGPD. Es en el consentimiento de los menores de edad donde se da la principal novedad. Si bien el RGPD establecía la edad mínima en 16 años para que el consentimiento resulte lícito, deja cierto margen a los Estados miembros para bajar esa cifra. Así, en artículo 7, se fija el límite en los 13 años, mínimo permitido por el Reglamento. Este hecho supone una modificación respecto a la LOPD de 1999, que lo fijaba en 14 años.

El Título IV contiene una serie de tratamientos que el legislador establece una presunción de prevalencia del interés legítimo del responsable si se dan ciertos requisitos. Es preciso recordar que el interés legítimo es una de las bases jurídicas válidas para que un tratamiento sea lícito, es decir, no le hace falta al responsable obtener el consentimiento del interesado para tratar sus datos. De este modo, se regulan más detalladamente que en la RGPD casos como la videovigilancia y sus requisitos para que se considere lícita, siempre con la finalidad de preservar la seguridad de las personas, bienes o instalaciones.

Una importante novedad respecto a la anterior LOPD consiste en la no inscripción de los ficheros de datos en el registro de la AEPD. Esta medida de control se transforma en el registro de actividades de tratamiento, visto en el RGPD.

Una de las importantes novedades respecto al RGPD consiste en la mayor precisión, mediante ejemplos prácticos, de cuales empresas están obligadas a nombrar un delegado de protección de datos y qué circunstancias en los tratamientos requieren de una evaluación de impacto. Ambos aspectos dan lugar a confusión en el Reglamento, pues se acogen a términos escasos y demasiado generalistas, como el de “a gran escala”. ¿Cuándo o qué cantidad se considera gran escala? Los especiales riesgos a tener en cuenta para la evaluación de impacto se recogen en el artículo 28.2 del Proyecto de ley, mientras que las diversas entidades obligadas a nombrar la figura del DPD se encuentran en artículo 34.1. Puede ver el proyecto en el siguiente enlace: *Acceso al Proyecto de ley*

En un modo de actuación similar al anterior visto, la nueva LOPD es más específica y práctica que el RGPD en el régimen sancionador, exponiendo de forma más detallada las distintas infracciones y a qué categoría de gravedad pertenecen.

Es preciso recordar que la nueva LOPD aún está en proceso de tramitación, por lo que todas estas matizaciones comentadas pueden cambiar, o bien surgir otras nuevas.

4 ESTUDIO DEL GRADO DE CUMPLIMIENTO DEL RGPD EN EL SECTOR DE LA ELECTRÓNICA DE CONSUMO EN ESPAÑA

En el presente capítulo se tratará el Reglamento General de Protección de Datos desde un punto de vista más práctico. Vistas ya detenidamente cada una de sus modificaciones y novedades incorporadas, se procederá a realizar un estudio de su influencia real en varias empresas pertenecientes al sector de la electrónica de consumo, comprobando como estas se adaptan y cumplen, si es el caso, las nuevas obligaciones en materia de protección de datos.

4.1 METODOLOGÍA Y LIMITACIONES

El fin principal de este capítulo consiste en la comprobación práctica y real de lo que ha supuesto para las empresas la llegada del RGPD. El estudio se realiza una vez absorbidos por parte del alumno los conceptos que rodean a esta cambiante materia, para garantizar un desarrollo del estudio más adecuado y una comprobación e interpretación de los resultados más correcta y exacta.

La metodología desarrollada, en términos generales, consiste en la verificación de una serie de elementos previamente establecidos -novedades incorporadas por el RGPD- en el ámbito de unas empresas elegidas mediante un proceso muestral -posicionamiento web-.

Los diferentes aspectos que componen este estudio serán comentados con mayor grado de detalle en la siguiente exposición de limitaciones:

1. **Las empresas estudiadas.** Resulta, lógicamente imposible, analizar todas las empresas que quedan sujetas al RGPD, más aún tras su ampliación en el ámbito territorial, afectando también a empresas no establecidas en Europa. Por tanto, una primera criba resulta ser empresas establecidas en España.

Sin embargo, el número de empresas sigue siendo desproporcionado. En acuerdo con el tutor del presente trabajo, se estableció la elección de un sector en concreto, con el objetivo de delimitar la cantidad posible de empresas a estudiar y permitir una mejor comparación de los resultados obtenidos. Las empresas mantendrán en común su actividad empresarial, por mucho que disten el resto de circunstancias, tamaño, etc.

El sector elegido es la electrónica de consumo. Este sector engloba empresas dedicadas a la venta y distribución de “todos los equipos electrónicos usados de manera cotidiana y que, generalmente, se utilizan para el entretenimiento, las comunicaciones y la oficina”. (ICEX, 2017) Ordenadores, smartphones, televisiones o cámaras de fotos son algunos de los más destacados. En consecuencia, se trata de un sector al alza, muy dinámico y con bajas barreras de entrada, lo cual el número de empresas a estudiar sigue siendo imposible a efectos técnicos en este trabajo.

Ante esta situación se presentó la idea de realizar la técnica de muestreo aleatorio estratificado, aplicado a las empresas de este sector establecidas en España, con el fin de obtener una muestra que fuese representativa y que incluyera en el análisis a empresas de distinto ámbito, desde pymes a empresas con sede en más países. No obstante, se demuestra la dificultad de aplicar este método, al no disponer de los recursos necesarios para hallar la Población del estudio, es decir, listado completo de todas las empresas del sector, añadiendo además el hecho de estar divididas para realizar la estratificación.

Como solución alternativa y final, se recurre al posicionamiento web. Así, mediante una serie de búsquedas en Google que contengan términos relacionados con el sector y sus productos, se realizará un listado con las empresas mejor posicionadas en los resultados naturales (SEO) en cada búsqueda. Este proceso será visualizado en el apartado siguiente.

2. Las novedades y modificaciones del RGPD a estudiar. La situación más deseable para el alumno en la ejecución de este estudio es, tras realizar una revisión pormenorizada de todas las novedades incluidas en el nuevo Reglamento, poder comprobar la influencia y grado de cumplimiento de todas y cada una de ellas que afectan en las distintas empresas a estudiar.

Sin embargo, este proceso no resulta posible, pues varias de las obligaciones impuestas a las empresas son de carácter interno, es decir, no es de ámbito público su elaboración y correspondiente cumplimiento. Tras intentos fallidos en establecer comunicación con las empresas seleccionadas, ha sido necesario modificar y adaptar los elementos de la lista deseados a nuestras circunstancias.

De este modo, el estudio se centrará principalmente en dos aspectos esenciales en la renovación llevada a cabo por el RGPD en materia de protección de datos, la mayor transparencia en la información dada a los individuos y en la obtención del consentimiento de los interesados. En próximos apartados será facilitada la lista con los elementos a verificar en las empresas objeto de estudio.

4.2 SELECCIÓN DE LA MUESTRA

A continuación, se procede a describir los términos utilizados para las correspondientes búsquedas y sus resultados, a fin de continuar el proceso de selección de las empresas a estudiar visto en el apartado anterior.

Es preciso señalar que las búsquedas “comprar electrónica de consumo” o “electrónica de consumo online” arrojaron resultados SEO poco adecuados a nuestro ámbito y alcance de estudio. Pese a ser el nombre propiamente del sector, las empresas no deciden posicionarse mediante estas palabras. Esto ocurre debido a la gran variedad de productos que integran el sector, que dejan a la electrónica de consumo en un lugar demasiado general, justificando el uso de términos más específicos e instaurados en la sociedad por parte de las empresas.

Olvidada la pretensión de que las empresas a analizar fuesen una muestra representativa del sector, optamos por otro método que, siendo conscientes de que no puede calificarse desde un punto de vista estadístico como científico, al menos nos permitiera obtener varias empresas para su análisis de forma sistemática. Optamos por usar cinco términos de búsqueda, siempre relacionados con el sector de la electrónica de consumo, y escoger la primera empresa¹ dedicada a la venta online que apareciese en los resultados naturales de Google.

Nuestro primer término de búsqueda fue “comprar informática”. La informática se puede englobar dentro de la electrónica de consumo, incluyendo ordenadores de sobremesa, portátiles, impresoras o tablets. A modo de ejemplo se adjunta la siguiente figura, con los tres primeros resultados obtenidos. Será seleccionada para el estudio la web *PcComponentes*.

¹ Posteriormente veremos que este criterio tuvo que ser modificado en la selección de las dos últimas empresas.



Figura 4.1. Búsqueda del término “comprar informática”

Fuente: resultados de una búsqueda en Google. A fecha de 28/06/2018

El segundo término objeto de estudio, similar al anterior, resulta ser “comprar productos informáticos”. Pese a su parecido, los resultados obtenidos distaban mucho de ser iguales. De esta búsqueda seleccionamos la web *Ecomputer*.

En vistas a seguir aumentando nuestro grado de especificación, el próximo término utilizado consiste en “comprar ordenadores portátiles”. Los resultados volvieron a situar al portal PcComponentes en primer lugar, por lo que nos quedamos con el segundo mejor posicionado, la web *Fnac*.



Figura 4.2. Búsqueda del término “comprar ordenadores portátiles”

Fuente: resultados de una búsqueda en Google. A fecha de 29/06/2018

El estudio de las pymes es fundamental en nuestra tarea de analizar el RGPD. Primeramente, debido a que conforman la gran parte del tejido empresarial español. Por otro lado, por el especial interés que promueve el hecho de tener que enfrentarse a esta

nueva normativa con unos recursos muy reducidos. En consecuencia, para los dos próximos términos se incluyó en las búsquedas la provincia local del alumno (Sevilla) a fin de conseguir unos resultados más ajustados a estas empresas de menor ámbito.

No obstante, esta inclusión no resultó plenamente satisfactoria, pues los resultados naturales de Google continuaban, en la mayoría de los casos, sin mostrar en el primer lugar a empresas de estas características, a causa de la escasa o nula inversión realizada en posicionamiento web por este tipo de empresas. Esta situación originó una modificación en el criterio de selección de la muestra, a fin de incluir a estas empresas en nuestro estudio, pasando a ser nuestra elección la primera pyme en aparecer en los resultados naturales de la búsqueda, y no el primer resultado como hasta ahora.

El cuarto término utilizado fue “comprar ordenadores smartphones en Sevilla”. Los smartphones son de los productos que mayor crecimiento han experimentado en los últimos años en la electrónica de consumo, por lo que merecían ser representados. La empresa *Tecnican* ha sido nuestra elección, posicionada en décimo lugar.

Tienda de informatica en Sevilla (Cantillana), telefonía, telefonos ...
<https://www.tecnican.com/> ▼
Accesorios para **ordenadores**, móviles, **smartphone**, tablet, smartwatch, tintas para impresoras HP, CANON, BROTHER, LEXMARK, RICOH, EPSON, periféricos ...

Búsquedas relacionadas con comprar smartphones ordenadores en sevilla

Figura 4.3. Búsqueda del término “comprar smartphones ordenadores en Sevilla”

Fuente: resultados de una búsqueda en Google. A fecha de 12/07/2018

Quinto y último término utilizado, hace referencia a “comprar informática en Sevilla”, donde la pyme seleccionada resulta ser *M. León Componentes Electrónicos*, posicionada en sexto lugar.

En conclusión, las empresas seleccionadas son:

- PC Componentes Y Multimedia S.L.U
- Ecomputer S.L
- Sociedad Grandes Almacenes Fnac España S.A.U
- Tecnican Servicios Informáticos de Cantillana.s.l
- Manuel Leon Gonzalez (Mleón Componentes Electrónicos)

4.3 ELABORACIÓN DE LA LISTA DE CONTROL

En el presente apartado se detallarán los distintos elementos a verificar su cumplimiento en las empresas objeto de estudio.

Es preciso recordar el carácter amplio del enfoque del riesgo impuesto por el RGPD, por el cual se acaban las listas cerradas de medidas de seguridad y las empresas, acorde a las categorías de datos que utilicen y el alcance de sus tratamientos, tomarán las medidas apropiadas que garanticen la seguridad de los datos. En consecuencia, las medidas adoptadas por una pyme para el cumplimiento del RGPD, son altamente probables que difieran de las adoptadas por una empresa con miles de empleados.

Una segunda precisión es el carácter interno de varias de las medidas, ya comentado en una de las limitaciones metodológicas. De este modo, aspectos tales como los contratos debidamente realizados entre responsable y encargado del tratamiento, o el registro de las actividades de tratamiento y las evaluaciones de impacto, no podrán ser analizados y, por tanto, verificado su cumplimiento en empresas que les sean obligatorios.

Los elementos de la lista de control estarán basados en aspectos más notorios y manifiestos del RGPD, la información prestada a los individuos y el proceso de obtención del consentimiento por parte del interesado. Ambos han visto como la transparencia juega un papel fundamental en sus respectivas renovaciones.

Respecto a la información prestada, se analizará principalmente el contenido del texto que haga referencia a la Política de Privacidad de la empresa, verificando que se dispone en él todos los elementos que el RGPD obliga a las empresas y con un lenguaje claro y sencillo. Para determinar los elementos que integran la lista, nos ayudamos de Figura 3.3. Información por capas, especialmente la 2ª capa o nivel.

En segundo lugar, durante el proceso de consentimiento del interesado, se observará que este exija una acción positiva, su lenguaje sea también claro y que cada tratamiento contemple su debido consentimiento por separado, si se diera el caso. Además, el consentimiento debe ser también informado, incorporando en el momento de la recogida de datos un enlace para revisar la Política de Privacidad o incluso mejor, aspectos de la primera capa de información. Figura 3.3. Información por capas

En resumen, los diferentes elementos a verificar son:

- La inclusión en la Política de Privacidad de la información adicional o de segunda capa de los diferentes epígrafes: responsable, finalidad, legitimación, destinatarios y derechos.
- Información accesible y fácil de entender, lenguaje claro y sencillo.
- Acción positiva en el consentimiento.
- Consentimiento informado, información de primera capa de los epígrafes citados arriba o enlace a la Política de Privacidad.

La lista de control quedaría compuesta por los siguientes elementos:

- ☐ Identidad y datos de contacto del responsable
- ☐ Identidad y datos de contacto del delegado de protección de datos
- ☐ Descripción de los fines del tratamiento
- ☐ Plazos o criterios de conservación de los datos
- ☐ Decisiones automatizadas, elaboración de perfiles
- ☐ Bases jurídicas detalladas de los tratamientos
- ☐ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☐ Destinatarios de los datos
- ☐ Previsión de transferencias, o no, a terceros países
- ☐ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☐ Derecho a retirar el consentimiento prestado
- ☐ Derecho a reclamar ante la autoridad de control
- ☐ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☐ Acción positiva requerida en el consentimiento
- ☐ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad

En caso de su correcta verificación, se utilizará el símbolo ☒.

En los casos que resultara negativo, el símbolo indicado es ☐.

Los aspectos más relevantes encontrados en cada empresa, ya sean positivos o negativos, pasarán a ser comentados.

4.4 REALIZACIÓN DEL ESTUDIO

En el presente apartado se llevará a cabo la realización del estudio introducido en este capítulo. Se adjuntarán, para una mayor claridad y dinamismo, capturas de las páginas web correspondientes a las empresas objeto de estudio. Finalmente, serán expuestas varias conclusiones acerca de los resultados obtenidos.

1. La primera empresa objeto de estudio es **PC Componentes Y Multimedia S.L.U.**

- ☒ Identidad y datos de contacto del responsable
- ☒ Identidad y datos de contacto del delegado de protección de datos
- ☒ Descripción de los fines del tratamiento
- ☐ Plazos o criterios de conservación de los datos
- ☐ Decisiones automatizadas, elaboración de perfiles
- ☒ Bases jurídicas detalladas de los tratamientos

- ☒ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☒ Destinatarios de los datos
- ☒ Previsión de transferencias, o no, a terceros países
- ☒ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☒ Derecho a retirar el consentimiento prestado
- ☒ Derecho a reclamar ante la autoridad de control
- ☒ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☒ Acción positiva requerida en el consentimiento
- ☒ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad



Figura 4.4. Política de Privacidad de PcComponentes

Fuente: <https://www.pccomponentes.com/privacidad>. A fecha de 03/07/2018.

La empresa contempla la figura del delegado de protección de datos, junto a una dirección de correo electrónico para su contacto. No obstante, la información no se presenta correctamente ordenada, pues su referencia se da en la parte final, lejos del epígrafe Responsable.

Respecto a la obligación o no de facilitar datos, en sus primeras líneas se dice “la visita a este sitio Web no implica que el usuario esté obligado a facilitar ninguna información. En el caso de que el usuario facilite alguna información de carácter personal, los datos recogidos en este sitio web serán tratados de forma leal y lícita”. No obstante, no se hace mención expresa a las consecuencias de no autorizar el tratamiento de datos.

En cuanto al consentimiento, este se presenta de una manera muy adecuada, cumpliendo todos los requisitos establecidos en el RGPD, especial mención la clara separación del tratamiento de envío de publicidad con su posible aceptación o no.



El formulario de creación de cuenta de PcComponentes está dividido en dos secciones principales: 'Entrar' y 'Nuevo cliente'. La sección 'Nuevo cliente' contiene un campo 'Soy:' con tres opciones de radio: 'Particular', 'Empresa u organización' y 'Autónomo'. Debajo de estas opciones, hay un texto que indica: 'Los campos marcados con * son obligatorios.' A continuación, hay dos campos de texto obligatorios: 'Email *' y 'Contraseña *'. Debajo de estos, hay una sección titulada 'Seguridad' con un subtexto: '* Utiliza 6 caracteres o más'. A continuación, hay un campo de texto obligatorio: 'Repetir contraseña *'. Finalmente, hay dos casillas de verificación: la primera es 'He leído y acepto la política de privacidad.' y la segunda es 'Me gustaría recibir descuentos exclusivos, novedades y tendencias por e-mail. Puedo darme de baja cuando quiera.' Ambas casillas están desmarcadas. Al final del formulario, hay un botón naranja que dice 'Crear cuenta'.

Figura 4.5. Obtención del consentimiento de PcComponentes

Fuente: <https://www.pccomponentes.com/login>. A fecha de 03/07/2018

2. La segunda empresa objeto de estudio es **Ecomputer S.L.**

- ☒ Identidad y datos de contacto del responsable
- ☒ Identidad y datos de contacto del delegado de protección de datos
- ☒ Descripción de los fines del tratamiento
- ☒ Plazos o criterios de conservación de los datos
- ☒ Decisiones automatizadas, elaboración de perfiles
- ☒ Bases jurídicas detalladas de los tratamientos
- ☒ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☒ Destinatarios de los datos
- ☒ Previsión de transferencias, o no, a terceros países
- ☒ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☒ Derecho a retirar el consentimiento prestado
- ☒ Derecho a reclamar ante la autoridad de control
- ☒ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☒ Acción positiva requerida en el consentimiento
- ☒ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad

POLITICA DE PRIVACIDAD

¿Quién es el responsable del tratamiento de datos personales?

Ecomputer S.L., con C.I.F. número **B22258982** y domicilio Parque Tecnológico Walqa, Edificio 5, CP: 22197, Huesca, teléfono 902220230 y correo electrónico protecciondedatos@ecomputer.es.

¿Con que finalidad se tratan los datos personales?

Ecomputer S.L., trata la información que se facilita con el fin de prestarle el servicio del cumplimiento de la relación contractual establecida en las relaciones de comercio electrónico, además de la gestión administrativa de la empresa.

Los datos personales proporcionados se conservarán mientras se mantenga la relación de prestación del servicio, hasta que solicite la supresión por parte del interesado o durante los años necesarios para cumplir con las obligaciones legales.

¿Se enviará información comercial?

Figura 4.6. Política de Privacidad de Ecomputer

Fuente: <https://tienda.ecomputer.es/content/8-politica-de-privacidad>. A fecha de 03/07/18

Esta Política de Privacidad está igualmente bien redactada y estructurada, siguiendo el orden expreso dado por la AEPD.

La empresa si hace referencia al plazo o criterios de conservación de los datos: “Los datos personales proporcionados se conservarán mientras se mantenga la relación de prestación del servicio, hasta que solicite la supresión por parte del interesado o durante los años necesarios para cumplir con las obligaciones legales”.

En esta empresa no se contempla la figura del delegado de protección de datos. A ciencia cierta, no se puede afirmar si esta empresa está obligada o no a tenerlo y su correspondiente incumplimiento de la normativa, pues a falta de una legislación más sólida en este tema, habría que valorar el alcance o “escala” -según dispone el RGPD- de sus tratamientos.

En referencia al consentimiento, a primera vista este no parece muy correcto y adecuado respecto a lo que el RGPD quiere. Pese a la acción afirmativa necesaria y el enlace a la información pertinente de protección de datos, el lenguaje utilizado parece demasiado explícito y breve.

CREAR UNA CUENTA

Escriba su correo electrónico para crear su cuenta

Correo electrónico

☐ He leído y acepto la [política de privacidad](#)



CREAR UNA CUENTA

Figura 4.7. Obtención del consentimiento de Ecomputer

Fuente: <https://tienda.ecomputer.es/inicio-sesion?back=my-account>. A fecha de 03/07/18

No obstante, si introducimos el correo electrónico se abre una nueva pantalla con una información y formato más acorde, donde se insertan el resto de datos personales.

Tratamiento

☐ Sr.

☐ Sra.

Nombre *

Apellido *

Correo electrónico * 

Contraseña * (Mínimo 5 caracteres)

Fecha de nacimiento

Tipo de cliente:

☐ Empresa

☒ Particular

☐ Distribuidor

En cumplimiento del Reglamento General de Protección que exige recabar un consentimiento explícito e inequívoco para cada tratamiento de datos, le informamos que marcando la casilla "Autorizo el envío de información comercial" nos facilita su consentimiento expreso para efectuar actividades de marketing y envíos de newsletter con información comercial y promociones

Figura 4.8. Seguimiento del proceso de obtención del consentimiento de Ecomputer

Fuente: <https://tienda.ecomputer.es/inicio-sesion?back=my-account#account-creation>. A fecha de 03/07/18

3. La tercera empresa objeto de estudio es **Sociedad Grandes Almacenes Fnac España S.A.U.**

- ☒ Identidad y datos de contacto del responsable
- ☒ Identidad y datos de contacto del delegado de protección de datos
- ☒ Descripción de los fines del tratamiento
- ☒ Plazos o criterios de conservación de los datos
- ☒ Decisiones automatizadas, elaboración de perfiles
- ☒ Bases jurídicas detalladas de los tratamientos
- ☒ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☒ Destinatarios de los datos
- ☒ Previsión de transferencias, o no, a terceros países
- ☒ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☒ Derecho a retirar el consentimiento prestado
- ☒ Derecho a reclamar ante la autoridad de control
- ☒ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☒ Acción positiva requerida en el consentimiento
- ☒ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad

8 . Política de privacidad

¿Quién es el responsable del tratamiento de sus datos personales?

El responsable del tratamiento de los datos será la Sociedad Grandes Almacenes Fnac España S.A.U, con N.I.F A80500200 y domicilio sito en el Parque Empresarial La Finca, Paseo de la Finca 1, bloque 11, 2ª planta, 28223, Pozuelo de Alarcón, Madrid. (en adelante e indistintamente "FNAC" o la "Entidad"). Para la adecuada gestión en el tratamiento de sus datos personales, FNAC tiene designado un Delegado de Protección de datos ante el que podrá acudir para resolver cualquier cuestión que precise, pudiendo contactar a través de la presente URL <https://gdpr.fnac.es/dpo.html>.

¿Con qué finalidades se tratan sus datos personales?

En FNAC podemos tratar los datos personales recabados para las siguientes finalidades:

1. Contacto: gestionar los datos de los usuarios que contactan con FNAC a través del formulario de contacto que la Entidad pone a disposición del usuario. Asimismo, sus datos serán tratados con el fin de gestionar las consultas que usted nos haga llegar a través de los canales habilitados a tal efecto en nuestra página web.
2. Trabaja con nosotros: gestionar la recepción de su Currículum Vitae, su candidatura, así como los datos personales que en su caso se generen como consecuencia de la participación en procesos de selección, con la finalidad de analizar su perfil profesional y de posibilitarle la participación en los procesos de selección de personal organizados por FNAC a la vista de los puestos vacantes o de nueva creación que se originen periódicamente; así como tramitar su eventual incorporación en plantilla de la Entidad. Le informamos que conservaremos sus datos por un periodo de tiempo no superior a un año por si en el futuro entendemos que encaja en alguno de los perfiles de empleo existentes.
3. Registro en el área de cliente "Fnac.es": gestionar su registro en la "Cuenta Fnac.es" así como los datos posteriores que se pudieran generar a través del citado canal, con la finalidad de llevar a cabo una administración general, mantenimiento, cumplimiento, desarrollo, control y gestión de las gestiones que usted realice a través de su Cuenta Fnac.es, así como de la gestión de su relación con la Entidad.

Figura 4.9. Política de Privacidad de Fnac

Fuente: https://www.fnac.es/condiciones_generales#punto8. A fecha de 05/07/2018

Esta empresa contiene la Política de Privacidad más extensa y detallada de las estudiadas, si bien es la que posee más recursos para su consecución y más tratamientos realiza.

Fnac sí contempla la elaboración de perfiles: "Perfilado basado en sus compras: siempre y cuando usted nos autorice, FNAC elaborará perfiles en base a estudios de marketing y técnicas y procedimientos estadísticos..." aspecto no visto en las otras empresas. No obstante, tampoco incorpora en el epígrafe Legitimación la obligatoriedad o no de facilitar datos y consecuencias de no hacerlo.

El aspecto más revolucionario de Fnac lo encontramos en la figura del delegado de protección de datos. El DPD goza de una página web propia, muy intuitiva donde el interesado puede ejercitar por separado cada uno de sus derechos, además de ponerse en contacto para la realización de consultas. Sin duda esta medida de Fnac va en consonancia con el principio de responsabilidad proactiva del RGPD. La protección de datos, realizada de esta manera, puede que suponga en un futuro no muy lejano una ventaja competitiva respecto a competidores que no la tengan tan presente en su política empresarial.



fnac FNAC - RGPD

| | |
|--|---|
| DERECHO DE ACCESO Utilice este formulario para ejercer su derecho de acceso sobre sus datos personales según la LOPD y el RGPD. | DERECHO DE RECTIFICACIÓN Utilice este formulario para ejercer su derecho de rectificación sobre sus datos personales según la LOPD y el RGPD. |
| DERECHO DE CANCELACIÓN Utilice este formulario para ejercer su derecho de cancelación de sus datos personales según la LOPD y el RGPD. | DERECHO DE OPOSICIÓN Utilice este formulario para ejercer su derecho de oposición a sus datos personales según la LOPD y el RGPD. |
| PORTABILIDAD DE DATOS PERSONALES Utilice este formulario para ejercer su derecho de portabilidad sobre sus datos personales según el RGPD. | LIMITACIÓN DE ACCIONES SOBRE DATOS PERSONALES Utilice este formulario para ejercer su derecho de limitación de acciones sobre sus datos personales según el RGPD. |
| CONSULTAS AL DPO Utilice este formulario para ponerse en contacto con el DPO de FNAC para cualquier consulta relativa al RGPD. | |

Figura 4.10. Delegado de Protección de Datos de Fnac

Fuente: <https://gdpr.fnac.es/>. A fecha de 05/07/2018

En cuanto al proceso de obtención del consentimiento realizado por Fnac, lo lleva a cabo de distinta forma que las demás empresas estudiadas. FNAC introduce información explícita directamente en el formulario de obtención del consentimiento, incorporando en ella otros enlaces que dispongan de mayor grado de detalle. Está formula de información por capas es la más recomendada por la AEPD.

☐ Quiero recibir información sobre las mejores ofertas y las promociones exclusivas de Fnac

☐ Marcando esta casilla, acepto y reconozco haber leído las **Condiciones Generales de Venta de Fnac.es** y las **Condiciones Generales de Venta de Marketplace**

Crear cuenta

Le informamos que sus datos serán tratados por Grandes Almacenes FNAC España S.A.U. (a partir de ahora "FNAC") que actuará en calidad del responsable del tratamiento de los mismos. Las finalidades de dichos tratamientos son el mantenimiento de la relación comercial y los servicios ofrecidos o contratados asociados a dicha relación. También se realizará el envío de comunicaciones comerciales de productos y servicios tanto de FNAC como de terceros. La base legitimadora de estos tratamientos es la propia obligación comercial. La base legitimadora del envío de comunicaciones comerciales tanto propias como de terceros, es el propio consentimiento explícito recogido en este mismo documento. Los datos personales se conservarán durante la vigencia de la relación comercial y posteriormente, siempre que el cliente no haya ejercitado su derecho de supresión, serán conservados teniendo en cuenta los plazos legales que resulten de aplicación en cada caso concreto, teniendo en cuenta la tipología de los datos, así como la finalidad del tratamiento. FNAC no realiza cesiones de los datos de carácter personal de sus clientes a ninguna otra entidad, salvo obligación legal que así lo disponga. FNAC garantiza al titular el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad dirigiéndose por escrito y acompañando fotocopia del DNI al Comité de Protección de Datos de Grandes Almacenes Fnac España, S.A.U., Paseo de la Finca 1, bloque 11, planta 2, 28223, Pozuelo de Alarcón, Madrid, o bien a través de vía electrónica en los formularios dispuestos en <https://gdpr.fnac.es/>. Para mayor información sobre el tratamiento de sus datos de carácter personal, puede dirigirse a la Política de privacidad de FNAC, alojada en la página web www.fnac.es. Asimismo, le informamos que FNAC ha nombrado un Delegado de Protección de Datos (DPO/DPD) que podrá contactarse a través de <https://gdpr.fnac.es/dpo.html> para cualquier información adicional al respecto.

Figura 4.11. Obtención del consentimiento de Fnac

Fuente: <https://secure.fnac.es/account/register>. A fecha de 06/07/2018

4. La cuarta empresa objeto de estudio es **Tecnican Servicios Informáticos de Cantillana.s.l.**

- ☒ Identidad y datos de contacto del responsable
- ☒ Identidad y datos de contacto del delegado de protección de datos
- ☒ Descripción de los fines del tratamiento
- ☒ Plazos o criterios de conservación de los datos
- ☒ Decisiones automatizadas, elaboración de perfiles
- ☒ Bases jurídicas detalladas de los tratamientos
- ☒ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☒ Destinatarios de los datos
- ☒ Previsión de transferencias, o no, a terceros países
- ☒ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☒ Derecho a retirar el consentimiento prestado
- ☒ Derecho a reclamar ante la autoridad de control
- ☒ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☒ Acción positiva requerida en el consentimiento
- ☒ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad

Política de Privacidad

En cumplimiento del artículo 5 de la Ley Orgánica 15/1999 de Protección de Datos, que regula el derecho de información en la recogida de los datos, ponemos en su conocimiento que los datos personales aportados por usted en nuestros formularios se incorporarán al fichero automatizado de Tecnican inscrito en la Agencia Española de Protección de Datos que contiene los datos de las personas que se han registrado a través de la página web.

La finalidad de la creación, existencia y mantenimiento de este fichero es el tratamiento de los datos de las personas que se han registrado en la página web de Tecnican con la exclusiva finalidad de llevar a cabo la gestión contable, fiscal y administrativa de los clientes que realizan compraventas on line. Los destinatarios de sus datos son el personal de Tecnican.

Así mismo, le informamos que Tecnican puede quedar obligada a ceder sus datos a la Administración Tributaria, para dar cumplimiento a las obligaciones fiscales,

Figura 4.12. Política de Privacidad de Tecnican

Fuente: <https://www.tecnican.com/privacy>. A fecha de 12/07/2018

Ya en sus primeras palabras deja prever su falta de adaptación al RGPD, siendo nombrada la LOPD de 1999. Bien por desconocimiento de la nueva normativa, falta de recursos o simplemente la oposición a realizarlo, la empresa está completamente desactualizada en la información prestada a los individuos en materia de protección de datos. Por lo tanto, puede enfrentarse a duras sanciones.

Los pocos aspectos que esta Política de Privacidad cumple son los ya contemplados por la LOPD, tales como identidad del responsable o fines del tratamiento.

Respecto a su proceso de obtención del consentimiento, la empresa esta vez sí cumple adecuadamente con lo impuesto por el RGPD.



The screenshot shows a registration form for 'Tecnican'. It includes two password fields: '* Contraseña' and '* Confirmar contraseña'. Below these is a 'Boletín de noticias' (Newsletter) section with a 'Subscribir' button and radio buttons for 'Si' and 'No'. At the bottom, there is a checkbox for 'He leído y estoy de acuerdo con la Política de Privacidad' and a 'Continuar' button.

Figura 4.13. Obtención del consentimiento de Tecnican

Fuente: <https://www.tecnican.com/index.php?route=account/register>. A fecha de 12/07/2018

5. La quinta y última empresa objeto de estudio es **Manuel Leon Gonzalez (Mleón Componentes Electrónicos)**.

- ☒ Identidad y datos de contacto del responsable
- ☒ Identidad y datos de contacto del delegado de protección de datos
- ☒ Descripción de los fines del tratamiento
- ☒ Plazos o criterios de conservación de los datos
- ☒ Decisiones automatizadas, elaboración de perfiles
- ☒ Bases jurídicas detalladas de los tratamientos
- ☒ Obligación o no de facilitar datos y consecuencias de no hacerlo
- ☒ Destinatarios de los datos
- ☒ Previsión de transferencias, o no, a terceros países
- ☒ Cómo ejercerlos derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento
- ☒ Derecho a retirar el consentimiento prestado
- ☒ Derecho a reclamar ante la autoridad de control
- ☒ Información accesible y fácil de entender, lenguaje claro y sencillo
- ☒ Acción positiva requerida en el consentimiento
- ☒ Consentimiento separado e informado, información de primera capa o enlace a la Política de Privacidad

POLÍTICA DE PRIVACIDAD

Declaración de privacidad de MLEON

Debido a la aplicación de la Nueva Normativa Europea para proteger la privacidad de los clientes y el correcto uso de sus datos (RGPD) a partir del 25 de mayo de 2018, nuestros términos de protección de datos cambian.

1 – RESPONSABLE

- Titular: MANUEL LEON CONZALEZ (MLEÓN COMPONENTES ELECTRÓNICOS) (en adelante, "MLEÓN COMPONENTES ELECTRÓNICOS")

Figura 4.14. Política de Privacidad de Mleón

Fuente: <https://mleon.com/politica-de-privacidad/>. A fecha de 12/07/2018

Esta pyme si cumple con creces su deber de informar. La información está muy bien estructurada, clara y completa. Este punto puede suponer una ventaja competitiva respecto a sus inmediatos competidores, pues la transparencia y seguridad ofrecida le facilitará ganarse la confianza de sus clientes y atraer a compradores potenciales.

Esta empresa sí contempla el aspecto informativo de la obligación o no de facilitar datos y consecuencias de no hacerlo, siendo una excepción al resto de empresas estudiadas. Así, en el epígrafe Legitimación se dicta: “el tratamiento de los datos del Usuario para gestionar, tramitar y dar seguimiento a las compras realizadas por el Usuario es la ejecución del contrato de compraventa, por lo que el suministro de los datos con este fin es obligado e impediría su cumplimiento en caso contrario.

Respecto al consentimiento, llama la atención la inexistencia de la casilla que haga referencia al envío de publicidad. La empresa marca en su Política de Privacidad: “para el envío de comunicaciones comerciales, para la elaboración de perfiles y para la realización de encuestas de satisfacción está basado en el **interés legítimo...**”. Suponiendo que las citadas comunicaciones comerciales son vía e-mail, esta es una medida errónea, ya que las comunicaciones comerciales realizadas por medios electrónicos están reguladas por la Ley 34/2002 de Servicios de la Sociedad de la Información, la cual exige en su artículo 21 el consentimiento expreso del destinatario. (Mediano, 2017)



The screenshot shows a web form for account creation. At the top, there is a text input field labeled 'Mi dirección'. Below it, a horizontal dashed line separates the header from the main content. The main content area has a title 'Privacidad de los datos del cliente' in blue. Underneath the title, there is a small square checkbox followed by a button labeled 'Política de privacidad de datos'. At the bottom right of the form, there is a large grey button labeled 'Registrarse'.

Figura 4.15. Obtención del consentimiento de Mleón

Fuente: <https://shop.mleon.com/autenticacion?back=my-account#account-creation>. A fecha de 12/07/2018

Tras la finalización del estudio, se exponen las siguientes conclusiones:

- No hay dos empresas iguales. Ninguna de las empresas coincide totalmente en los elementos de la lista de control verificados.
- No hay empresa que cumpla todos los elementos. Este hecho, junto al expuesto anteriormente, da a entender la difusa y complicada tarea que es la protección de datos para las empresas en su conjunto.
- No parece simplemente una cuestión de recursos. Hemos observado como la quinta empresa objeto de estudio, la empresa Mleón Componentes Electrónicos, cumplía casi en su totalidad las medidas impuestas por el RGPD, pese a ser una pyme con un solo establecimiento en Sevilla.

La mayor concienciación social acerca de la protección de datos personales, fundamentalmente desde el punto de vista del interesado y la preocupación por su propia seguridad, junto a las primeras sanciones impuestas por la Agencia Española de Protección de Datos, estimularán progresivamente a las empresas a un mayor grado de acción en materia de protección de datos. La repetición de este estudio pasados unos meses puede dar lugar a unos resultados considerablemente distintos.

5 Conclusiones

La realización del presente Trabajo Fin de Grado ha supuesto un reto mayúsculo para el alumno. El primer enfrentamiento a un trabajo de tales características siempre es duro, especialmente en los inicios.

El elevado desconocimiento general sobre el tema a tratar fue el primer inconveniente al que el alumno debió de enfrentarse, solventándolo con el paso de los días a causa de numerosas investigaciones. El proceso de ejecución del trabajo ha sido largo, pero siempre didáctico y entretenido, avanzando con el tiempo ambos aspectos de menos a más.

El escaso conocimiento de la rama del Derecho resultó otra de las primeras limitaciones para el alumno. Acudir en los inicios a los textos jurídicos con el objetivo de generar conocimientos sobre el tema fue un error, pues el lenguaje utilizado en estos textos escapaba de las habilidades del alumno. Ante ello, se consultaron otras fuentes de información que mezclaran el rigor requerido con un lenguaje más inteligible.

El alumno obtiene, con la realización de este trabajo, una base en materia de protección de datos bastante competente que podrá aplicar en el ámbito empresarial, ya sea desde el papel de cliente, vigilando su propia seguridad, o desde la perspectiva de la búsqueda de empleo.

La continua renovación es el principal atributo que hace este tema tan atractivo. Su velocidad de cambios es tal que nuestro objeto central de estudio, el Reglamento General de Protección de Datos, acaba de entrar en aplicación y ya cabe la posibilidad de considerarlo ciertamente obsoleto, al no estar adaptados plenamente a sistemas como el Big Data.

En conclusión, la experiencia ha resultado muy provechosa a todos los niveles. La protección de datos es un tema muy relevante en nuestra sociedad actual, y el cual no hará más que crecer, pues sigue el ritmo de los avances tecnológicos. Esto da al alumno una visión de futuro, en un tema que no quiere perder el contacto y seguirá realizando futuras investigaciones y formándose.

6 Bibliografía

- Agencia Española de Protección de Datos. (2005). Guía del derecho fundamental a la protección de datos de carácter personal. Recuperado de https://portal.uah.es/portal/page/portal/proteccion_datos/repositorio/guiadelaagencia.pdf
- Agencia Española de Protección de Datos. (2017a). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. Recuperado de <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>
- Agencia Española de Protección de Datos. (2017b). Protección de Datos: Guía para el Ciudadano. Recuperado de <https://www.aepd.es/media/guias/guia-ciudadano.pdf>
- Agencia Española de Protección de Datos. (2017c). Guía para el cumplimiento del deber de Informar. Recuperado de <https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf>
- Agencia Española de Protección de Datos. (2018). Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD. Recuperado de <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>
- Anciano, C. (16 de marzo de 2015). Diferencia entre intimidad y privacidad. Recuperado de <http://loquelaleyregula.blogspot.com/2015/03/diferencia-entre-intimidad-y-privacidad.html>
- Baquía. (2 de marzo de 2006). Intimidad, privacidad y protección de datos de carácter personal. Recuperado de <https://www.baquia.com/emprendedores/intimidad-privacidad-y-proteccion-de-datos-de-caracter-personal>
- Barbará, Á. (26 de febrero de 2018). Llegan fechas clave para la protección de datos en España. Recuperado de <https://www.saberespractico.com/investigacion/apa/referenciar-una-pagina-web-en-apa/>

- Canales, Á. (2007, abril). El derecho fundamental a la protección de datos de carácter personal. Revista jurídica de Castilla y León. Recuperado de <https://dialnet.unirioja.es/servlet/articulo?codigo=2280278>
- Carta de los derechos fundamentales de la Unión Europea. (DOUE núm. 364, 18 de diciembre de 2000).
- “conceptodefinicion.de”. (Sin fecha). Definición de Reglamento. Recuperado de <http://conceptodefinicion.de/reglamento/>
- Constitución Española. (BOE núm. 311, 29 de diciembre de 1978).
- Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. (BOE núm. 274, de 15 de noviembre de 1985).
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE núm. 281, de 23 de noviembre de 1995).
- Enmiendas e índice de enmiendas al articulado 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. (Boletín Oficial de las Cortes Generales núm. 13-2, 18 de abril de 2018).
- Enmienda (ley). (Sin fecha). En Wikipedia. Recuperado el 25 de junio de 2018 de [https://es.wikipedia.org/wiki/Enmienda_\(ley\)](https://es.wikipedia.org/wiki/Enmienda_(ley))
- “eur-lex.europa.eu”. (Sin Fecha, a). Protección de los datos personales. Recuperado de <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=LEGISSUM:l14012>
- “eur-lex.europa.eu”. (Sin Fecha, b). Glosario de las síntesis: Instrumentos jurídicos de la UE. Recuperado de https://eur-lex.europa.eu/summary/glossary/community_legal_instruments.html?locale=es
- ICEX España Exportación e Inversiones. (Mayo de 2017). La electrónica de consumo, un sector en alza en Eslovaquia. Recuperado de <https://www.icex.es/icex/es/navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/paises/navegacion-principal/noticias/NEW2017712421.html?idPais=SK>
- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. (BOE núm. 262, de 31 de octubre de 1992)

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (BOE núm. 298, 14 de diciembre de 1999)
- Maeztu, D. (8 de diciembre de 2015). La historia del artículo 18.4 de la Constitución. Recuperado de <http://www.derechoynormas.com/2015/12/la-historia-del-articulo-184-de-la.html>
- Martínez de Pisón, J. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. Anuario De Filosofía Del Derecho, pp.409-430.
- Mayor, R. (2016, junio). Contenido y novedades del Reglamento General de Protección de Datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). Revista del Gabinete Jurídico de Castilla-La Mancha. Recuperado de <https://dialnet.unirioja.es/servlet/articulo?codigo=5698351>
- Mediano, S. (16 de octubre de 2017). Informe AEPD sobre aspectos relativos al Reglamento Europeo de Protección de Datos. Recuperado de <http://www.santiagomediano.com/informe-aepd-sobre-aspectos-relativos-al-reglamento-europeo-de-proteccion-de-datos/>
- Noguer, A. (14 de febrero de 2018). RGPD (II): Transferencia internacional de datos. Recuperado de <http://www.eljurista.eu/2018/02/14/rgpd-ii-transferencia-internacional-de-datos/>
- Oltra, J.V. (28 de enero de 2016). Historia de la protección de datos personales | UPV [Archivo de vídeo]. Recuperado de: <https://www.youtube.com/watch?v=S7uXyCyOwyw>
- Oltra, J.V. (4 de octubre de 2017). Historia de la protección de datos en el siglo XX | UPV [Archivo de vídeo]. Recuperado de: <https://www.youtube.com/watch?v=wlfAldZrWww>
- Pavón, J.A. (2001-2002). La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. Anuario de la Facultad de Derecho (Universidad de Extremadura), pp. 235-252.
- Piñar, J.L. (mayo-diciembre 2003). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. Cuadernos de Derecho Público, núms. 19-20.

- Piñar, J.L. (Dir.) , Álvarez, M. (coord.), Recio, M. (coord.). (2016). Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos. Barcelona, España: Editorial Reus.
- Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal 121/000013. (Boletín Oficial de las Cortes Generales núm. 13-1, 24 de noviembre de 2017).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (BOE núm. 17, de 19 de enero de 2008).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (DOUE núm. 59, de 4 de mayo de 2016).
- San José, C. (30 de enero de 2018). Los principios del Reglamento (UE) General de Protección de Datos (y 5); en particular, el de integridad y confidencialidad. Recuperado de <https://esaged.wordpress.com/2018/01/30/los-principios-del-reglamento-ue-general-de-proteccion-de-datos-y-5-en-particular-el-de-integracion-y-confidencialidad/>
- Universitat de València. (Sin fecha). ¿Cuándo entran en vigor las normas? Recuperado de https://www.uv.es/legalskills/validez/cundo_entran_en_vigor_las_normas.html
- Vázquez, S., y de Miguel, J. (2017, junio). Nuevo régimen sancionador de protección de datos. Economist & Jurist. Recuperado de <https://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf>